



OpenText™ Server Backup - Public Cloud

Administrator Guide

Copyright 2025 Open Text

Server Backup - Public Cloud Administrator Guide revision Thursday, November 20, 2025.

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

One or more patents may cover this product. For more information, please visit <https://www.opentext.com/patents>.

For terms and conditions, see [Terms and Conditions](#).

Version History

Version	Date	Description
1	November 2025	Initial guide for Server Backup - Public Cloud.

Table of Contents

1 Introduction to Server Backup - Public Cloud	5
1.1 Account types and permissions	5
2 Starting a trial or subscription	7
2.1 Starting a trial or subscription in Secure Cloud	7
2.2 Data deletion after a trial or subscription ends	9
3 Setting up Server Backup storage	10
3.1 Amazon S3 buckets for Server Backup storage	13
3.2 Permissions for creating the IAM role using a CloudFormation template	13
3.3 AWS IAM role for Server Backup agents	15
3.3.1 IAM role requirements	16
3.3.2 Trust policy	16
3.3.2.1 Using the same storage for multiple Management Consoles	17
3.3.3 Permissions policy	18
3.3.3.1 Updating the IAM role for new S3 buckets	20
3.4 Detecting unexpected S3 cost spikes with AWS Cost Anomaly Detection	22
3.5 Viewing and managing storage information	22
3.6 Adding S3 buckets for Server Backup	23
3.7 Validating S3 buckets for Server Backup data	24
3.8 Removing Server Backup access to S3 buckets	24
4 Viewing and managing Server Backup policies	26
4.1 Viewing and editing Server Backup policies	26
4.2 Adding a Server Backup policy	29
4.3 Retention settings	31
4.4 Deleting a Server Backup policy	32
4.5 Changing a device's Server Backup policy	33
4.6 Changing a site's Server Backup policy	34
5 Installing and managing agents	35
5.1 Downloading and installing the Windows Agent	35
6 Managing devices, backups and recoveries	37
6.1 Running unscheduled backups	40
6.2 Monitoring or stopping a backup	41
6.3 Changing an agent password	41
6.4 Deleting a device or canceling a deletion	42
7 Monitoring Server Backup	44
7.1 Monitoring Server Backup using the dashboard	44
7.2 Setting up email notifications	45
8 Viewing and exporting Server Backup reports	47
8.1 Server Backup reports	48

9 Recovering files and folders	50
10 Recovering volumes	52
11 Recovering servers after a disaster	54
11.1 Recovering a Windows server to hardware or to a virtual machine	54
11.1.1 Downloading the BMR Media Creator	55
11.1.2 Creating recovery media	55
11.1.3 Obtaining a disaster recovery code	57
11.2 Recovering Windows servers to the AWS cloud	58
11.2.1 Starting a recovery to the AWS cloud	59
11.2.2 AWS IAM role for recovering servers to the AWS cloud	61
11.2.3 Decommissioning AWS resources after recovery	65
11.3 Recovering a Windows server	66
11.3.1 Choosing a recovery server	69
11.3.2 Automatically mapping drives in a recovery	70
11.3.3 Manually mapping drives in a recovery	71
11.3.4 Source and recovery server icons	74
11.3.5 Setting up a network connection for the BMR Agent	76
11.3.6 Installing or updating device drivers	77
11.3.7 Configuring recovery log settings	79
11.3.8 Running Windows utilities from a command prompt	80
11.3.9 System-specific recovery information	80
11.3.9.1 Recovering UEFI-based systems	80
11.3.9.2 Recovering BIOS-based systems	81
11.3.9.3 Recovering systems with OEM partitions	82
11.3.9.4 Recovering servers with device installation restrictions	82
11.3.9.5 Recovering dynamic disks and spanned volumes	83
11.4 Repairing a recovered server	85
11.4.1 Items in the Repair wizard	87
11.5 Recovering Active Directory servers: Enabling AD authentication for recovered servers via AWS VPN	88
11.5.1 Prerequisites	88
11.5.2 Setting up the AWS AD Connector	88
11.5.3 Configuring the AWS Client VPN Endpoint with AD Authentication	89
12 Supported platforms and system requirements	90
12.1 Windows Agent supported platforms, requirements and recommendations	90
12.2 BMR Media Creator supported platforms, requirements and known issues	92
12.3 BMR Agent supported platforms, requirements and known issues	94

1 Introduction to Server Backup - Public Cloud

With OpenText Server Backup - Public Cloud, you can quickly and securely back up your servers to cloud storage, and recover files, volumes and servers when you need them.

To ensure that backups run quickly, Server Backup - Public Cloud only backs up new and changed data after the initial "seed" backup. All backup data is encrypted in transit and at rest, and only you know the password required to restore it.

In the event of a threat such as ransomware, hardware failure, or a natural disaster, you can recover exactly what you need— specific files and folders, selected volumes, or entire servers.

You can manage Server Backup - Public Cloud using the same platform used to manage other OpenText threat prevention and security solutions. Using this suite of cybersecurity products, you can defend your systems against threats and recover data quickly if a problem occurs.

Getting started

To start backing up data using Server Backup - Public Cloud, do the following:

1. Start a free Server Backup trial or buy a subscription. If you manage products for multiple customers or sites, you can start a separate Server Backup trial or subscription for each customer or site. See *Starting a trial or subscription* on page 7.

When you start a trial or subscription, you choose a storage location for the backup data and select a policy with a schedule for backing up data.

2. Install the Server Backup agent on each server or device where you want to back up data. See *Installing and managing agents* on page 35.

The agent automatically starts backing up data as specified by its storage location and policy. You can then:

- Manage backups, recoveries, and devices where the Server Backup agent is installed. See *Managing devices, backups and recoveries* on page 37.
- Run unscheduled backups. See *Running unscheduled backups* on page 40.
- Recover files and folders, volumes, or entire servers. See *Recovering files and folders* on page 50, *Recovering volumes* on page 52, or *Recovering servers after a disaster* on page 54.

Note: Your account type and site permissions determine which Server Backup tasks you can perform. For more information, see *Account types and permissions* below.

1.1 Account types and permissions

Your account type and roles determine which Server Backup tasks you can perform.

If you are a partner administrator with the Administrator or Sales role in Secure Cloud, you can do the following:

- Start Server Backup trials and subscriptions for customers.
- View and manage Server Backup devices in customer sites.
- Create and manage global and site Server Backup policies.
- Set up and manage storage for Server Backup data.

If you are a partner administrator with the Support role in Secure Cloud, you cannot start Server Backup trials and subscriptions, but you can do the following:

- View and manage Server Backup devices in customer sites.
- Create and manage global and site Server Backup policies.
- Set up and manage storage for Server Backup data.

If you are a customer administrator in Secure Cloud, you cannot start Server Backup trials or subscriptions or set up storage. However, you can do the following:

- View and manage Server Backup devices in your site
- Create and manage Server Backup policies in your site.

If you are a Secure Cloud user who does not have Administrator permissions, you cannot view or manage Server Backup trials, subscriptions, devices, policies, or storage.

2 Starting a trial or subscription

To start backing up data using Server Backup - Public Cloud, you must start a free Server Backup trial which can later be converted into a subscription. If you manage products for multiple customers, you can start a separate trial or subscription for each customer or site. See *Starting a trial or subscription in Secure Cloud* below.

During a free 30-day trial, you can use all Server Backup functionality. You can install the Server Backup agent on an unlimited number of servers, back up and restore data, monitor processes, and run reports. You can upgrade the trial to a paid subscription at any time and continue backing up servers without reconfiguring backups.

When you start a trial or subscription, you must choose a storage location for the backup data and a policy with settings for Server Backup agents. If you have not set up cloud storage for Server Backup, you are prompted to set it up at this time. See *Setting up Server Backup storage* on page 10.

After starting a trial or subscription, you can install the Server Backup agent on each server or device where you want to back up data. The agent then contacts the Management Console to obtain its site's storage location and policy, and automatically starts backing up data as specified by the storage location and policy. See *Installing and managing agents* on page 35.

2.1 Starting a trial or subscription in Secure Cloud

If you manage products for multiple customers using Secure Cloud, you can start a separate Server Backup trial for each customer. Each trial can be converted to a subscription when the trial ends, or you can cancel the trial.

When you start a Server Backup - Public Cloud trial, you must:

- Choose a storage location for the backup data. You cannot change the storage location for a site after it is selected.

If Server Backup storage has not been set up when you start a trial, a message banner prompts you to set it up. See *Setting up Server Backup storage* on page 10.

- Choose a Server Backup policy for agents in the site. The policy provides settings for Server Backup agents, including a schedule for backing up data and retention settings that specify how long to keep each backup.

Note: To provide different settings for a specific agent, you can assign a different policy to the device where the agent is installed. This is useful, for example, if you want the agent to back up data at a different time than other agents in its site. See *Changing a device's Server Backup policy* on page 33.

IMPORTANT: If a trial ends without being converted to a subscription, or a subscription is not renewed, the customer's backup data will be automatically deleted after a grace period. For more information, see *Data deletion after a trial or subscription ends* on page 9.

To start a Server Backup trial or subscription in Secure Cloud:

1. When signed in to Secure Cloud as a partner administrator with the Administrator or Sales role, go to **Partner Services > Customer Management > Product catalog** and start a Server Backup trial for a customer.

For more information, see Secure Cloud videos and documentation, or contact your service provider for assistance.

Note: Each Server Backup subscription begins as a trial which can later be converted to a subscription.

2. Click **Home**.

A task on the home page indicates that Server Backup must be set up for the customer.

3. In the Server Backup task, click the menu button **...**, and then click **Explore** to view more information. In the task information, click **Manage**.

4. Read the setup steps, and then click **Setup Server Backup**.

The Server Backup tab for the customer's site opens in the Management Console. If a message banner prompts you to set up Server Backup cloud storage, you must set up the storage before setting up the trial or subscription. See *Setting up Server Backup storage* on page 10.

5. Select the backup storage location for the customer's site.

IMPORTANT: You cannot change the backup storage location after selecting it.

6. Select the Server Backup policy for devices in the site.

The policy provides settings such as a schedule for backing up data and retention settings that specify how long to keep each backup. For more information, see *Viewing and managing Server Backup policies* on page 26

7. Click **Save**.

You can then install Server Backup agents and start backing up servers. See *Installing and managing agents* on page 35.

2.2 Data deletion after a trial or subscription ends

If a Server Backup trial ends without being converted to a subscription, a Server Backup subscription is not renewed, or a site is deactivated, the backup data for the customer or site is deleted after a grace period.

There is a 7-day grace period after a trial expires or is disabled or suspended. If a customer converts their trial to a subscription before the end of the grace period, the customer's backup data remains and they can recover from existing backups. If a customer does not convert their trial to a subscription within 7 days after the trial ends, the customer's backup data is deleted. If the customer purchases a subscription after the grace period, they must start over with a new backup storage location and new backups.

There is a 30-day grace period after a subscription expires or is disabled or suspended. If a customer renews their subscription before the end of the grace period, the customer's backup data remains and they can recover from existing backups. If a customer does not renew their subscription within 30 days after the subscription ends, the customer's backup data is deleted. If the customer purchases a subscription after the grace period, they must start over with a new backup storage location and new backups.

Note: Backups do not run during the 7-day grace period after a trial ends or the 30-day grace period after a subscription ends.

Note: If a site is deleted from the Management Console, its backups are immediately marked for deletion from cloud storage. There is no grace period after a site deletion.

Note: There is sometimes a delay before backup data is deleted from storage. Depending on the amount of data, it can take several days to delete the data. You cannot recover device data during this time.

3 Setting up Server Backup storage

Server Backup agents back up data to and restore data from Amazon Simple Storage Service (Amazon S3) in your Amazon Web Services (AWS) account.

When you first start a Server Backup trial or subscription in the Management Console, you are prompted to set up the storage. During the setup, you must:

- Enter your AWS account number.
- Specify one or more Amazon S3 buckets for Server Backup data. Each bucket must already exist in your AWS account. For requirements, see *Amazon S3 buckets for Server Backup storage* on page 13. We recommend adding one bucket for each physical region that you support. For example, you could add one bucket in the United States, and one bucket in Europe. Multiple customers can back up data to the same S3 bucket, but each customer can only access their own data.
- Create an AWS Identity and Access Management (IAM) role in your AWS account that allows Server Backup agents to back up data to and restore data from the specified S3 buckets. We recommend creating the IAM role using a CloudFormation template that you download from the Management Console, but you can also create the IAM role using the AWS Management Console, an IaC product such as Terraform, or another method. For IAM role requirements, see *AWS IAM role for Server Backup agents* on page 15.

You can pause the storage setup process at any time. Information that you have entered will be saved so you can resume the setup later.

You cannot change the AWS account for storing Server Backup data after it is set up in the Management Console. However, if you manage Server Backup for multiple customers or sites, you can add additional S3 buckets for storing Server Backup data. See *Adding S3 buckets for Server Backup* on page 23.

To set up Server Backup storage:

1. After a Server Backup - Public Cloud trial is created in Secure Cloud, a task on the Home page prompts you to complete setup steps. In the task, click **Explore** and then click **Manage**.
2. On the **System Setup** tab, after reviewing setup steps, click **Setup server backup**.
You are directed to the customer's Server Backup tab in the Management Console.
3. If a message banner prompts you to set up Server Backup cloud storage, click **Setup** in the message banner.

Note: You can also click **Server Backup** in the navigation pane, and then click **Set up** on the Server Backup information page.

4. In the **Server Backup Guided Setup: Backup Storage** wizard, enter information on the following pages:

Note: If the storage setup was paused before it was complete, the wizard starts on the next page where information is required. To pause the storage setup, click **Finish Later** on any page in the wizard.

- a. On the **Cloud Account** page, do the following and then click **Next**:
- In the **Friendly Name** box, type a name for the cloud storage account. This storage account name appears in the Management Console and does not have to match your account name in AWS.
 - (Optional) In the **Description** box, type a description of the cloud storage account.
 - In the **AWS Account ID** box, type your 12-digit AWS Account ID.

SERVER BACKUP GUIDED SETUP: BACKUP STORAGE

- b. On the **Backup Storage** page, in the S3 Bucket box, type the name of each S3 bucket where you want to store Server Backup data. Separate multiple bucket names with commas or spaces, or press Enter after typing each bucket name. Click **Next**.

The S3 buckets must already exist in your Amazon S3 account, and must meet the requirements listed in *Amazon S3 buckets for Server Backup storage* on page 13.

You can also add additional S3 buckets after the initial cloud storage setup. See *Adding S3 buckets for Server Backup* on page 23.

- c. On the **IAM Role** page, do one of the following to create an IAM role in your AWS account that allows Server Backup agents to access specified S3 buckets:

- (Recommended) To create the IAM role using a CloudFormation template, click **Download Template**.

You can then sign in to your AWS account and, in the AWS CloudFormation console, create a stack with the IAM role using the downloaded template. For the stack name, use any name that has not been used previously. You must have permissions in AWS to create the stacks using CloudFormation templates. For more information, see *Permissions for creating the IAM role using a CloudFormation template* on the next page.

IMPORTANT: If you are an administrator for an MSP or partner with more than one Management Console, and want to use the same AWS account for all of your Server Backup storage, only download and use a CloudFormation template when setting up storage in your first console. When setting up storage in additional consoles or adding S3 buckets, do not download a CloudFormation template. Instead, edit the IAM role manually. See *AWS IAM role for Server Backup agents* on page 15.

- To create the required role in your AWS account without using a CloudFormation template, record the **External ID**.

You can then create the IAM role in your AWS account using the AWS Management Console, an IaC product such as Terraform, or another method. For IAM role requirements, see *AWS IAM role for Server Backup agents* on page 15.

Note: If you need time to create the IAM role, click **Finish Later** to pause the storage setup. When you start the storage setup again, the wizard starts on the next page where information is required.

After you create the IAM role for Server Backup agents, select **I have created/updated the IAM role in the AWS management console**, and then click **Next**.

- d. On the **Validation** page, check whether the IAM role allows access to each S3 bucket. Do one of the following:

- If an S3 bucket validation fails, click **Failed** in the **Status** column to view error information.

After making required changes, click **Refresh validation** to check the IAM role again.

- If an S3 bucket validation status is **Passed**, click **Save**.

When at least one S3 bucket passes validation, you can set up Server Backup trials and subscriptions for sites. See *Starting a trial or subscription in Secure Cloud* on page 7.

3.1 Amazon S3 buckets for Server Backup storage

Before you set up Server Backup storage in the Management Console, you must create at least one Amazon S3 bucket in your AWS account for Server Backup storage. An S3 bucket that is used for Server Backup storage should not be used for any other workloads.

Requirements and recommendations for S3 buckets for Server Backup are listed below. During the storage setup, each S3 bucket is validated to ensure that it meets all requirements and can be accessed by Server Backup agents. Validation fails if an S3 bucket does not have the required settings. Validation does not fail if an S3 bucket does not have the recommended settings.

Amazon S3 bucket requirements and recommendations

Amazon S3 bucket characteristic or property	Value	Required or recommended
AWS Region	Any region in the aws partition	Required
Bucket Name	Any name that complies with Amazon S3 bucket naming rules	Required
Object Ownership	ACLs disabled	Recommended
Block Public Access	Block <i>all</i> public access	Recommended
Bucket Versioning	Enabled	Required
Object Lock	Enabled	Required
Requester pays	Disabled	Required
Static website hosting	Disabled	Required

We do not recommend enabling an Intelligent-Tiering rule for an S3 bucket for Server Backup data. If an S3 bucket has an Intelligent-Tiering rule (for example, moving data to Amazon S3 Glacier storage in 30 days instead of the default of 90), validation will fail for the S3 bucket.

We recommend adding one S3 bucket for each physical region that you support. For example, you could add one bucket in the United States, and one bucket in Europe. Multiple customers can back up data to the same S3 bucket, but each customer can only access their own data.

3.2 Permissions for creating the IAM role using a CloudFormation template

To create the IAM role that allows Server Backup agents to access your S3 buckets, we recommend downloading a CloudFormation template from the Management Console and using the template to create a stack in the AWS CloudFormation console. To do this, you must have AWS permissions to create and update stacks, work with S3 buckets, and manage IAM roles.

The following sample shows possible permissions for setting up Server Backup storage using a downloaded CloudFormation template. To determine the permissions you require, consult with an AWS power user in your organization or see documentation from Amazon Web Services.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Allow",
      "Action": [
        "cloudformation:CreateStack",
        "cloudformation:CreateUploadBucket",
        "cloudformation>DeleteStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "cloudformation:ListStacks",
        "cloudformation:UpdateStack",
        "cloudformation:CreateChangeSet",
        "cloudformation:GetTemplateSummary",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ListChangeSets",
        "cloudformation:ExecuteChangeSet",
        "s3:PutBucketObjectLockConfiguration",
        "s3:PutBucketVersioning",
        "s3:CreateBucket",
        "s3:PutObject",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutBucketPolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:AttachRolePolicy",
        "iam:CreateInstanceProfile",
        "iam:CreatePolicy",
        "iam:CreatePolicyVersion",
        "iam:CreateRole",
```

```
        "iam:DeleteInstanceProfile",
        "iam:DeletePolicyVersion",
        "iam:DeleteRole",
        "iam:DetachRolePolicy",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:ListRoles",
        "iam:PassRole",
        "iam:PutRolePolicy",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:UpdateAssumeRolePolicy"
    ],
    "Resource": ["*"]
}
]
```

3.3 AWS IAM role for Server Backup agents

Server Backup data is stored in one or more Amazon S3 buckets in your AWS account. To allow Server Backup agents to access your S3 buckets, you must create an IAM role in your AWS account. Server Backup agents can assume this role and back up data to and restore data from your S3 buckets.

To create the IAM role, we recommend downloading a CloudFormation template from the Management Console and using the template to create a stack in the AWS CloudFormation console. See *Setting up Server Backup storage* on page 10. Alternatively, you can create the IAM role in your AWS account using the AWS Management Console, an IaC product such as Terraform, or another method.

IMPORTANT: If you are an administrator for an MSP or partner with more than one Management Console, and want to use the same AWS account for all of your Server Backup storage, do not download a CloudFormation template when setting up storage in additional consoles or adding S3 buckets. Instead, edit the IAM role trust policy or permissions policy manually. See *Using the same storage for multiple Management Consoles* on page 17 and *Updating the IAM role for new S3 buckets* on page 20.

If you add a bucket to your Server Backup storage, you must update the IAM role in your AWS account so that Server Backup agents can back up data to and restore data from the new S3 bucket. See *Updating the IAM role for new S3 buckets* on page 20.

3.3.1 IAM role requirements

The IAM role in your AWS account must meet the following requirements:

- The role name must be: `ServerBackupAccessRole`
- The maximum session duration, in seconds, must be: 21600
- The trust policy must allow Server Backup agents to assume the `ServerBackupAccessRole` role in your AWS account. For trust policy requirements in JSON format, see *Trust policy* below.
- The permissions policy must allow the trusted role to read and write data in the Amazon S3 buckets where you want to store Server Backup data. For required permissions in JSON format, see *Permissions policy* on page 18.

3.3.2 Trust policy

The following trust policy in JSON format is required for Server Backup agents to back up data to and restore data from your Amazon S3 buckets. Server Backup agents are trusted to access your storage and are identified by the `"arn:aws:iam:662124509659:role/OpenTextServerBackupAccessAssumeRole"` role.

The trust policy must specify the External ID from the Server Backup Guided Setup wizard in the Management Console. In the following example, the External ID is `12345678-abcd-1234-abcd-12345678910a`. Replace this value with your External ID from the Server Backup Guided Setup wizard. For more information, see *Setting up Server Backup storage* on page 10.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS":
"arn:aws:iam::662124509659:role/OpenTextServerBackupAccessAssumeRole"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
```



```
        "StringEquals": {
            "sts:ExternalId": "12345678-abcd-1234-abcd-12345678910a"
        }
    },
    {
        "Effect": "Allow",
        "Principal": {
            "AWS":
"arn:aws:iam::662124509659:role/OpenTextServerBackupAccessAssumeRole"
        },
        "Action": "sts:TagSession"
    }
]
```

3.3.2.1 Using the same storage for multiple Management Consoles

If you are an admin for an MSP or partner with more than one Management Console, and want to use the same AWS account for all of your Server Backup storage, only download and use a CloudFormation template to set up storage for the first console. For subsequent consoles, copy the External ID from the Server Backup Guided Setup wizard and manually add it in the IAM role trust policy in your AWS account.

In the following example, the External ID for the second console is 98765432-dcba-9876-dcba-98765432110d.

```
{
    "Effect": "Allow",
    "Principal": {
        "AWS":
"arn:aws:iam::662124509659:role/OpenTextServerBackupAccessAssumeRole"
    },
    "Action": "sts:AssumeRole",
```

```
    "Condition": {
      "StringEquals": {
        "sts:ExternalId": [
          "12345678-abcd-1234-abcd-12345678910a",
          "98765432-dcba-9876-dcba-98765432110d"
        ]
      }
    }
  }
}
```

3.3.3 Permissions policy

The following permissions policy in JSON format is required for Server Backup agents to back up data to and restore data from your Amazon S3 buckets.

The permissions policy must specify the name of each S3 bucket where agents can read and write data. In the following example, the S3 buckets are named "bucket-one" and "bucket-two". Replace these names with your own S3 bucket names.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "BucketLevelPermissions",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:GetBucketVersioning",
        "s3:ListBucketVersions",
        "s3:GetIntelligentTieringConfiguration",
        "s3:PutIntelligentTieringConfiguration",
        "s3:GetLifecycleConfiguration",

```

```
        "s3:PutLifecycleConfiguration",
        "s3:GetBucketObjectLockConfiguration",
        "s3:PutBucketObjectLockConfiguration"
    ],
    "Resource": [
        "arn:aws:s3:::bucket-one",
        "arn:aws:s3:::bucket-two"
    ]
},
{
    "Sid": "ObjectLevelPermissions",
    "Effect": "Allow",
    "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:GetObjectAttributes",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionAttributes",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:BypassGovernanceRetention",
        "s3:GetObjectLegalHold",
        "s3:GetObjectRetention",
        "s3:PutObjectLegalHold",
        "s3:PutObjectRetention"
    ],
    "Resource": [
        "arn:aws:s3:::bucket-one/*",
        "arn:aws:s3:::bucket-two/*"
    ]
}
]
```

3.3.3.1 Updating the IAM role for new S3 buckets

If you add an Amazon S3 bucket to your Server Backup storage, you must update the IAM role in your AWS account so that Server Backup agents can back up data to and restore data from the new S3 bucket. To do this, you can download a CloudFormation template from the Management Console and use the template to update the IAM role in your AWS account. See *Adding S3 buckets for Server Backup* on page 23.

IMPORTANT: If you are an administrator for an MSP or partner with more than one Management Console, and use the same AWS account for all of your Server Backup storage, do not download and use a CloudFormation template when adding S3 buckets in your consoles. Instead, edit the IAM role permissions policy manually, as described below.

You can also manually add the buckets to the two resource lists in the permissions policy. For example, if you add an S3 bucket named "bucket-three", add its name in both resource lists in the permissions policy as shown below.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "BucketLevelPermissions",
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation",
                "s3:GetBucketVersioning",
                "s3:ListBucketVersions",
                "s3:GetIntelligentTieringConfiguration",
                "s3:PutIntelligentTieringConfiguration",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:GetBucketObjectLockConfiguration",
                "s3:PutBucketObjectLockConfiguration"
            ],
            "Resource": [
                "arn:aws:s3:::bucket-one",
                "arn:aws:s3:::bucket-two",
```

```
        "arn:aws:s3:::bucket-three"
    ]
},
{
    "Sid": "ObjectLevelPermissions",
    "Effect": "Allow",
    "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:GetObjectAttributes",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionAttributes",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:BypassGovernanceRetention",
        "s3:GetObjectLegalHold",
        "s3:GetObjectRetention",
        "s3:PutObjectLegalHold",
        "s3:PutObjectRetention"
    ],
    "Resource": [
        "arn:aws:s3:::bucket-one/*",
        "arn:aws:s3:::bucket-two/*",
        "arn:aws:s3:::bucket-three/*"
    ]
}
]
```

3.4 Detecting unexpected S3 cost spikes with AWS Cost Anomaly Detection

Unexpected increases in Amazon S3 storage or data transfer costs can occur if excessive or unintended data is written to your S3 buckets. While the data itself remains securely protected through encryption and AWS access controls, these events can lead to significant and unexpected charges if not promptly identified.

We recommend configuring AWS Cost Anomaly Detection to automatically monitor your S3-related costs. The service uses machine learning to learn your typical cost patterns and alerts you when storage or data egress spending diverges from normal trends. By creating a cost monitor scoped to the S3 service, you can receive timely alerts through email or Amazon SNS and take quick action to investigate the source of the anomaly.

For full setup instructions, see AWS Cost Anomaly Detection information in the AWS documentation. It outlines how to create monitors, configure alert subscriptions, and view detected anomalies in the AWS Billing Console.

3.5 Viewing and managing storage information

If storage for Server Backup data is set up in your Management Console, you can:

- View storage information.
- Change the name and description of the storage.
- Validate existing S3 buckets to ensure that they meet all requirements and can be accessed by Server Backup agents.

You can also add additional S3 buckets for storing backup data. See *Adding S3 buckets for Server Backup* on the next page.

You cannot change the Server Backup storage for a site after it is selected.

To view and manage storage information:

1. In the navigation pane, go to **Server Backup > Backup Storage**.

The **Backup Storage** page shows information about where your backup data is stored.

Note: If you cannot access this page, Server Backup storage is not set up in your Management Console or you do not have permission to manage Server Backup storage. For more information, see *Setting up Server Backup storage* on page 10.

2. To edit the storage account name or description, do the following:
 - a. (Optional) In the **Friendly Name** box, type a name for the cloud storage account. This name appears in the Management Console and does not have to match your account name in AWS.
 - b. (Optional) In the **Description** box, type a description of the cloud storage account.
 - c. Click **Save**.

3. To validate an S3 bucket, in the Actions menu  for the S3 bucket, click **Validate**.

If the S3 bucket validation fails, click **Failed** in the **Status** column to view error information. Check that the bucket meets the requirements listed in *Amazon S3 buckets for Server Backup storage* on page 13 and can be accessed using the role created in *Setting up Server Backup storage* on page 10.

3.6 Adding S3 buckets for Server Backup

If you manage Server Backup for multiple customers or sites, you can add additional S3 buckets for Server Backup data after the initial storage setup. The S3 buckets must meet the requirements listed in *Amazon S3 buckets for Server Backup storage* on page 13.

After adding an S3 bucket, you must update the IAM role in your AWS account so that Server Backup agents can back up data to and restore data from the new S3 bucket.

To add S3 buckets for Server Backup:

1. In the navigation pane, go to **Server Backup > Backup Storage**.

If you cannot view this page, storage for Server Backup data is not set up in your Management Console or you do not have permission to manage Server Backup storage. For more information, see *Setting up Server Backup storage* on page 10 or *Account types and permissions* on page 5.

2. Click **Add Backup Storage**.
3. On the **Backup Storage** page, in the S3 Bucket(s) box, type the name of each S3 bucket that you want to add for storing Server Backup data. Separate multiple bucket names with commas or spaces, or press Enter after typing each bucket name. Click **Next**.

Only enter S3 bucket names that already exist in your Amazon S3 account. Each bucket must meet the requirements described in *Amazon S3 buckets for Server Backup storage* on page 13.

4. On the **IAM Role** page, do one of the following to update the IAM role in your AWS account that allows Server Backup agents to access specified S3 buckets:

- To update the IAM role using a CloudFormation template, click **Download Template**.

You can then sign in to your AWS account and use the downloaded template to update the IAM role. To do this, in the AWS CloudFormation console, make a direct update to your previously-created stack and replace the existing template with the template you just downloaded. For more information, see AWS CloudFormation documentation from Amazon Web Services. For permissions information, see *Permissions for creating the IAM role using a CloudFormation template* on page 13.

IMPORTANT: If you are an administrator for an MSP or partner with more than one Management Console, and use the same AWS account for all of your Server Backup storage, do not download and use CloudFormation templates when adding S3 buckets. Instead, update the IAM role manually. See *Updating the IAM role for new S3 buckets on AWS IAM role for Server Backup agents* on page 15.

- To update the required role in your AWS account without using a CloudFormation template, use the AWS Management Console, an IaC product such as Terraform, or another method to add the name of each new S3 bucket in the IAM role in your AWS account. For IAM role requirements, see *AWS IAM role for Server Backup agents* on page 15.
5. After you create the IAM role for Server Backup agents, select **I have created/updated the IAM role in the AWS management console**, click **Validate** and then check whether validation for each S3 bucket has passed.

If validation fails for an S3 bucket, click **Failed** in the **Status** column to view error information. Check that the bucket meets the requirements listed in *Amazon S3 buckets for Server Backup storage* on page 13 and can be accessed using the role created in *Setting up Server Backup storage* on page 10.


3.7 Validating S3 buckets for Server Backup data

You can validate existing S3 buckets to check that they can be used for Server Backup data.

To validate an S3 bucket for Server Backup data:

1. In the navigation pane, go to **Server Backup > Backup Storage**.

If you cannot view this page, storage for Server Backup data is not set up in your Management Console. For more information, see *Setting up Server Backup storage* on page 10.

2. In the **Backup Storage List**, find the S3 bucket that you want to validate. In the **Actions** menu  for the S3 bucket, click **Validate**.

If validation for the S3 bucket fails, check that the bucket meets the requirements listed in *Amazon S3 buckets for Server Backup storage* on page 13 and can be accessed using the role created in *Setting up Server Backup storage* on page 10.

3.8 Removing Server Backup access to S3 buckets

Partners who no longer want to offer Server Backup - Public Cloud to their customers can remove Server Backup access to their Amazon S3 buckets.

After a customer's Server Backup trial or subscription ends, there is a grace period before backup data is deleted from storage. See *Data deletion after a trial or subscription ends* on page 9. Because there can be a delay before backup data is deleted after a grace period, we recommend waiting to remove access to S3 buckets until a week after customers' grace periods end.

To remove Server Backup access to your Amazon S3 buckets, do one of the following:

- Delete the permissions policy from your AWS account that allows Server Backup agents to back up data to and restore data from your Amazon S3 buckets. For more information, see *AWS IAM role for Server Backup agents* on page 15.
- If you set up Server Backup storage using a CloudFormation template, delete the stack you created using the CloudFormation template. This will delete the *ServerBackupAccessPolicy*

policy that allows Server Backup agents to access your S3 buckets. See *Setting up Server Backup storage* on page 10.

4 Viewing and managing Server Backup policies

A Server Backup policy provides settings for Server Backup agents, including a schedule for backing up data and retention settings that specify how long to keep each backup. To view, edit, or add policies, see *Viewing and editing Server Backup policies* below or *Adding a Server Backup policy* on page 29.

When you start a trial or subscription for a customer or site, you must select a Server Backup policy for agents in the site. Server Backup agents then contact the Management Console, obtain their policy settings, and back up data as specified by the policy. See *Starting a trial or subscription in Secure Cloud* on page 7.

To change settings for Server Backup agents, you can do any of the following:

- Change the policy that is assigned to a site. See *Changing a site's Server Backup policy* on page 34
- Change the policy that is assigned to a device. See *Changing a device's Server Backup policy* on page 33.
- Edit settings in a policy that is assigned to one or more sites or devices. See *Viewing and editing Server Backup policies* below.

After you change the policy for a site or device, or edit a policy that is assigned to a site or device, agents obtain the new policy settings when they next contact the Management Console. Server Backup agents usually contact the Management Console once every hour.

4.1 Viewing and editing Server Backup policies

You can view policies that provide settings for Server Backup agents, including a schedule for backing up data and retention settings that specify how long to keep each backup.

There are three types of Server Backup policies:

- **System**— System policies are available for all sites and devices.
- **Global**— Global policies are available for sites where the **Include Global Policies** setting is enabled on the site's **Details** tab.
- **Site**— Site policies are only available for one site.

You can edit Global and Site policies. If you edit a policy that is assigned to one or more devices or sites, agents obtain the new policy settings when they next contact the Management Console. Server Backup agents usually contact the Management Console once every hour.

You cannot edit System policies. However, you can copy a System policy and edit settings in the new policy. See *Adding a Server Backup policy* on page 29.

To view and edit Server Backup policies:

1. In the navigation pane, go to **Server Backup > Policies**.

The **Policies** page lists available policies. The **Type** column indicates whether each policy is a System, Global or Site policy. The **Last Updated** column shows the last date and time when each Global and Site policy was updated. Times are shown in your user's time zone set in the Management Console.

2. To specify which policies appear in the list, do one of the following:
 - To view policies that are available for all sites, click **Global** in the **Policies** list.
 - To view policies that are available for a specific site, click the site name in the **Policies** list.
3. Click the name of the policy that you want to view or edit.

Note: You can edit Global and Site policies. You cannot edit System policies.

4. In the **Name** and **Description** boxes, view or edit the policy name and description.
5. In the **Policy Settings** area, view or edit policy settings in the following sections. To hide or show settings in a section, click the arrow beside the section name.

- **Basic Configuration**

Automatically download and upgrade agents	Specifies whether a Server Backup agent is upgraded automatically when a new agent version is available. If selected, the agent is upgraded automatically when a new agent version is available. If not selected, the agent is not upgraded automatically. When a new agent version is available, you must download the agent installer from the Management Console and manually upgrade the agent.
Run first backup after agent installation	Specifies whether a Server Backup agent backs up data immediately after it is installed on a device. If selected, the agent backs up device data immediately after it is installed. If not selected, the agent backs up device data at the first scheduled backup time.

- **Backup Content**

The Backup Content section specifies which data a Server Backup agent backs up on a device. For the current release, the only available setting is **Entire Server**. This means that an agent backs up all data on a device, including non-removable volumes that are added after the agent is installed. The agent sequentially backs up all blocks on each volume in a server rather than backing up specific files and folders.

- **Cloud Backup Schedule**

Backup Frequency	Specifies the time each day when an agent backs up device data. Backups run at the specified time according to the system time on the device where the agent is installed. If the device is not synchronized with an NTP server, the system time could be different than the real local time.
Backup Active Days	Specifies the days of the week when an agent backs up device data at the time specified by the Backup Frequency setting.
Automatically retry failed backups	Specifies whether scheduled backups automatically retry if they do not run successfully. If selected, scheduled backups retry after a failed backup attempt. The Retry failed backups box specifies the number of times that the backup should retry. The Wait before each retry attempt for [] minutes box specifies the number of minutes between backup attempts. If not selected, scheduled backups do not retry after a failed backup attempt.

- **Cloud Backup Retention**

Cloud Backup Retention settings specify how long to keep each backup before automatically deleting it. This minimizes the amount of storage used and reduces storage costs. For more information, see *Retention settings* on page 31.

Standard Retention	If selected, each backup is kept for 30 days and the first successful backup of each month is kept for 12 months.
Custom Retention	If selected, backups are kept as specified by the Keep Daily backups for , Keep Weekly backups for , Keep Monthly backups for , and Keep Yearly backups for boxes.

- **Backup Maintenance**

Run maintenance every day at	Specifies the time each day when maintenance processes run in Server Backup storage to delete backup data that is no longer required according to the agent's retention settings. Deleting backup data minimizes the amount of storage used and reduces storage costs.
-------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

6. In the **Policy Usage** area, view the sites and number of devices that use the policy.

For each site, the **Number of Endpoints** column shows the number of devices that use the policy, compared to the total number of devices in the site.

7. If you edited the policy, click **Save**.

4.2 Adding a Server Backup policy

You can add Global and Site policies that provide settings for Server Backup agents, including a schedule for backing up data and retention settings that specify how long to keep each backup. Global policies are available for sites where the **Include Global Policies** setting is enabled on the site's **Details** tab. Site policies are only available for one site.

You cannot add System policies, which are available for all sites and devices. However, you can copy a System policy and edit settings in the new policy.

To add a Server Backup policy:

1. In the navigation pane, go to **Server Backup > Policies**.
2. Do one of the following:
 - To add a policy that is not based on an existing policy, click **Add Policy**.
 - To copy an existing policy, find the policy with settings that you want to copy. In the **Actions** menu for the policy, click **Copy**.
3. In the **Name** and **Description** boxes, type a name and description for the new policy.

The policy name must be unique for the scope of the policy. For a global policy, the name must be unique across all sites. For a site policy, the name must be unique for the site.
4. In the **Scope** area, do one of the following:
 - To make the policy available to all sites that allow Global Policies, click **Global**. Global Policies are allowed for sites where the **Include Global Policies** setting is turned on the site's **Details** tab.
 - To make the policy available for one site, click **Site**. In the **Select a site** list, click the site for the policy.

Note: You cannot add a System policy. System policies are available for all sites and devices.
5. In the **Policy Settings** area, specify policy settings in the following sections. To hide or show settings in a section, click the arrow beside the section name.

- **Basic Configuration**

Automatically download and upgrade agents	<p>Specifies whether a Server Backup agent is upgraded automatically when a new agent version is available.</p> <p>If selected, the agent is upgraded automatically when a new agent version is available.</p> <p>If not selected, the agent is not upgraded automatically. When a new agent version is available, you must download the agent installer from the Management Console and manually upgrade the agent.</p>
Run first backup after agent installation	<p>Specifies whether a Server Backup agent backs up data immediately after it is installed on a device.</p> <p>If selected, the agent backs up device data immediately after it is installed.</p> <p>If not selected, the agent backs up device data at the first scheduled backup time.</p>

- **Backup Content**

The Backup Content section specifies which data a Server Backup agent backs up on a device. For the current release, the only available setting is **Entire Server**. This means that an agent backs up all data on a device, including non-removable volumes that are added after the agent is installed. The agent sequentially backs up all blocks on each volume in a server rather than backing up specific files and folders.

- **Cloud Backup Schedule**

Backup Frequency	<p>Specifies the time each day when an agent backs up device data.</p> <p>Backups run at the specified time according to the system time on the device where the agent is installed. If the device is not synchronized with an NTP server, the system time could be different than the real local time.</p>
Backup Active Days	<p>Specifies the days of the week when an agent backs up device data at the time specified by the Backup Frequency setting.</p>
Automatically retry failed backups	<p>Specifies whether scheduled backups automatically retry if they do not run successfully.</p> <p>If selected, scheduled backups retry after a failed backup attempt. The Retry failed backups box specifies the number of times that the backup should retry. The Wait before each retry attempt for [] minutes box specifies the number of minutes between backup attempts.</p> <p>If not selected, scheduled backups do not retry after a failed backup attempt.</p>

- **Cloud Backup Retention**

Cloud Backup Retention settings specify how long to keep each backup before automatically deleting it. This minimizes the amount of storage used and reduces storage costs. For more information, see *Retention settings* below.

Standard Retention	If selected, each backup is kept for 30 days and the first successful backup of each month is kept for 12 months.
Custom Retention	If selected, backups are kept as specified by the Keep Daily backups for , Keep Weekly backups for , Keep Monthly backups for , and Keep Yearly backups for boxes.

- **Backup Maintenance**

Run maintenance every day at	Specifies the time each day when maintenance processes run in Server Backup storage to delete backup data that is no longer required according to the agent's retention settings. Deleting backup data minimizes the amount of storage used and reduces storage costs.
-------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

6. Click **Save**.

4.3 Retention settings

To minimize the amount of storage used and reduce storage costs, Server Backup data that is no longer needed is automatically deleted from storage.

Retention settings in a Server Backup policy specify how long to keep each backup before maintenance processes delete the data.

If **Standard retention** is selected, the first backup of each day is kept for 30 days and the first backup of each month is kept for 12 months.

If **Custom retention** is selected, backups are kept as specified by the following values:

- **Keep daily backups for** specifies the number of days to keep each backup.
- **Keep weekly backups for** specifies the number of weeks to keep the first backup of each week, where a week starts on Monday. If **Not required** is selected, the first backup of each week is not kept for a specified amount of time.
- **Keep monthly backups for** specifies the number of months to keep the first backup of each month. If **Not required** is selected, the first backup of each month is not kept for a specified amount of time.
- **Keep yearly backups for** specifies the number of years to keep the first backup of each year, where a year begins on January 1. If **Not required** is selected, the first backup of each year is not kept for a specified amount of time.

The following table summarizes how long backups are kept, depending on your retention settings.

Note: Every backup, including unscheduled or "ad hoc" backups, is kept for at least 24 hours.

Backup Type	Description	Standard retention settings	Custom retention settings
Daily backup	First completed backup on a day.	Kept for 30 days	Kept for the number of days specified for daily backups in the custom retention settings
Weekly backup	First completed backup in a week, where a week begins on a Monday. If a backup is completed on a Monday, it is considered the weekly backup for the week. If there are no completed backups during a week, there is no weekly backup for the week.	No retention settings for weekly backups	Kept for the number of weeks specified for weekly backups in the custom retention settings
Monthly backup	First completed backup in a month. If weekly backups are kept, the first weekly backup of a month is considered the monthly backup. If weekly backups are not kept, the first completed backup of the month is considered the monthly backup.	Kept for 12 months	Kept for the number of months specified for monthly backups in the custom retention settings
Yearly backup	First completed backup in a year, where a year begins on January 1. If monthly backups are kept, the first monthly backup of the year is considered the yearly backup. If monthly backups are not kept, the first completed backup of the year is considered the yearly backup.	No retention settings for yearly backups	Kept for the number of years specified for yearly backups in the custom retention settings

Note: If only one backup remains for a device, it will not be deleted by maintenance processes. The last backup for a device is only deleted if you manually delete the device from the Management Console. See *Deleting a device or canceling a deletion* on page 42.

4.4 Deleting a Server Backup policy

You can delete a Server Backup policy. When deleting a policy, you can choose a replacement policy for sites and devices that use the policy you are deleting.

To delete a Server Backup policy:

1. In the navigation pane, go to **Server Backup > Policies**.
2. On the **Policies** page, click the name of the policy that you want to delete.

Note: You can only delete a policy that has the Global or Site scope. Policies with the System scope are available to all sites and devices and cannot be deleted.

3. On the **Server Backup Policy** page, click **Delete Policy**.
4. In the **Delete Server Backup Policy** box, in the **Replacement Policy** list, choose a replacement policy for sites and devices that use the policy you are deleting.
5. Click **Save**.

4.5 Changing a device's Server Backup policy

To change settings for a device where a Server Backup agent is installed, you can change the policy for the device. This is useful, for example, if you want the agent to back up data at a different time than specified by the default policy for agents in its site.

When the agent next contacts the Management Console, it obtains the new policy's settings and starts backing up data as specified by the new policy. Agents typically contact the Management Console once every hour.

You can also edit settings in a Global or Site policy that is assigned to the device. See *Viewing and editing Server Backup policies* on page 26.

To change a device's Server Backup policy:

1. In the navigation pane, go to **Server Backup > Devices**.
2. Do one of the following:
 - To change the policy for one device, click the name of the device.
 - To change the policy for one or more devices, select the check box for each device.

Note: You cannot change the Server Backup policy for a device that is scheduled for deletion.

3. Click **Change Policy**.
4. In the **Server Backup policy** list, do one of the following:
 - To specify a policy for the device or devices, select the policy name.
 - To have the device or devices inherit the site's Server Backup policy, select **Inherit Policy from site (*policyName*)**.

5. Click **Change Policy**.

A **Success** notification appears.

4.6 Changing a site's Server Backup policy

To change settings for Server Backup agents in a site, you can choose a different policy for the site. When an agent in the site next contacts the Management Console, it obtains the new policy's settings and starts backing up data as specified by the new policy. Agents typically contact the Management Console once every hour.

You can also edit settings in a Global or Site policy that is assigned to the site. For more information, see *Viewing and editing Server Backup policies* on page 26.

To change a site's Server Backup policy:

1. On the **Sites List**, click the name of the site for which you want to change the Server Backup policy.
2. On the site page, click the **Server Backup** tab.
3. In the **Server Backup policy** list, choose the policy for agents in the site.
4. Click **Save**.

A **Success** notification appears.

5 Installing and managing agents

After starting a Server Backup trial or subscription and choosing a storage location and policy for a customer or site, you can download the Server Backup - Public Cloud agent installer from the Management Console and install the agent on each device where you want to back up data. See *Downloading and installing the Windows Agent* below.

When you install the Server Backup agent, you must specify the keycode for its site. The agent then automatically starts backing up device data as specified by the site's storage location and policy. You can also run unscheduled backups. See *Running unscheduled backups* on page 40.

You can manage devices where Server Backup agents are installed on the **Devices** page. See *Managing devices, backups and recoveries* on page 37.

5.1 Downloading and installing the Windows Agent

You can download the Windows Agent installer from the Management Console and install it on each Windows server that you want to back up. Each server must meet the requirements listed in *Windows Agent supported platforms, requirements and recommendations* on page 90.

When you install an agent, you must specify a password for encrypting the agent data. This password is required for recovering the data, so be sure to keep it somewhere safe. You can change the password any time without reseeding the backup data. See *Changing an agent password* on page 41.

For best backup performance, the server must be restarted after the agent is installed. The server can restart automatically after the installation process is complete, or you can restart the server later.

To download the Windows Agent:

1. In the navigation pane, click **Sites List**. Click the name of the site for which you want to download the Windows Agent.
2. On the site's **Server Backup** tab, in the **Download Software** area, do the following:
 - Click **Download Windows Agent (.exe)**.
 - Copy and record the site's keycode. You must enter this keycode when installing the agent. The agent can then contact the console and start backing up the device as specified by the site's storage location and policy.

To install the Windows Agent:

1. On the Windows server that you want to back up, double-click the Windows Agent installation kit.
2. In the language list, click the language for the installer UI text, and then click **OK**.
3. If a message states that you must install required software, click **Install**.
4. On the **Welcome** page, click **Next**.

5. On the **Destination Folder** page, do one of the following:

- To install the agent in the default location, click **Next**.
- To install the agent in another location, click **Change**. In the **Change Current Destination Folder** dialog box, browse to the new installation folder, or enter it in the **Folder** name box. Click **OK**. On the **Destination Folder** page, click **Next**.

IMPORTANT: Do not install the Server Backup agent in a Windows-encrypted directory.

6. On the **Agent Password** page, do the following:

- a. In the **Password** and **Confirm Password** boxes, enter a password for encrypting and recovering the data. The password can have ASCII characters only, with no spaces or angled brackets < >. The following special characters are allowed: !"#\$%&'()*+,-./:;=?@[\]^_`{|}~

IMPORTANT: This password is required for recovering the data, so be sure to keep it somewhere safe. If you forget your password, you will not be able to restore your data. The password is not maintained anywhere else and cannot be recovered.

- b. (Optional) To check whether the password meets the password requirements, click **Test Password**. A message indicates whether the password meets the requirements. Click **OK**.
- c. Click **Next**.

7. On the **Register Agent with the Management Console** page, enter the keycode for the site. When the agent contacts the console, it will start backing up data as specified by the site's backup location and policy.

If you did not record the keycode when you downloaded the agent software, click **Sites List** in the Management Console and then click the site name. The keycode appears on the site's **Details** tab and the **Server Backup** tab.

8. Click **Install**.

9. In the **Server restart is recommended** box, do one of the following:

- To restart the server automatically immediately after the agent is installed, click **Yes**.
- To restart the server manually later, click **No**.

IMPORTANT: For best backup performance, the server must be restarted after the agent is installed.

10. On the **InstallShield Wizard Completed** page, click **Restart Server** or **Finish**.

After the agent is installed on the Windows server, the name of the server appears on the **Server Backup > Devices** page and you can manage the device and its backups. See *Managing devices, backups and recoveries* on page 37.

6 Managing devices, backups and recoveries

You can manage Server Backup devices, backups, and recoveries using the Devices page. You can view information about devices where Server Backup agents are installed, and manage backups and recoveries on the devices.




Note: After an event occurs on a device, there can be a delay of up to one minute before event information appears in the Management Console.

To manage devices, backups and recoveries:







1. In the navigation pane, go to **Server Backup > Devices**. The **Devices** page lists devices where Server Backup agents are installed.

(Optional) To view devices in a particular site, click the site name in the **Sites** list.

The **Name** column shows the name of each device where an agent is installed, and includes any of the following icons that apply:

-  Backup in progress – Indicates that the device is currently being backed up.
-  Reboot necessary for optimal backup performance – Indicates that the device needs to be restarted for backups to run efficiently. If you restart a Windows server after installing an agent on the server, the agent can use Changed Block Tracking (CBT) to identify data that has changed since the previous backup. If you do not restart the device, the agent cannot use CBT and must read all data when backing up the server.
-  Change indicator – Indicates that a change has occurred for the device, such as a policy change or scheduled deletion, but the change is not reflected on the Devices page yet.

The **Status** column shows one of the following statuses for each device:




-  **Protected** – The last backup completed successfully.
-  **Needs attention** – The last backup failed or did not run.
-  **Pending** – An agent is installed on the device but the first backup has not completed.
-  **Scheduled for Deletion** – The device is scheduled for deletion. To see when the device is scheduled to be deleted, point to the question mark  beside the **Scheduled for Deletion** status. For more information, see *Deleting a device or canceling a deletion* on page 42.
-  **Expired** – The Server Backup trial or subscription for the device's site has ended and Server Backup features are disabled. The site's backup data will be deleted if the subscription is not renewed within a grace period. For more information, see *Data deletion after a trial or subscription ends* on page 9.

Note: Canceled and in-progress backups are not considered when determining a device's status

The **Availability** column indicates whether each device is in contact with the Management Console:

- **Online** – The device is in contact with the console.
- **Offline** – The device is not currently in contact with the console. A device can be offline if it is turned off, if the agent has been uninstalled from the device, or if the system has been lost.

The **Site** column shows the site of each device. A device's site is determined by the site keycode that you enter when you install an agent on the device.

The **Policy** column shows the policy that is assigned to each device. If a site icon  appears beside a policy name, the policy is inherited from the device's site. If a computer icon  appears beside a policy name, the policy is assigned directly to the device. See *Changing a device's Server Backup policy* on page 33. If a question mark  appears beside a policy name, the policy is not applied to the device yet. The policy will be applied to the device when the next scheduled backup starts or within an hour if the device is online.

The **Last Seen** column shows the last time when each agent was in contact with the console. The time is shown in your user's time zone set in the Management Console.

The **OS** column shows the operating system of each device.

Note: The Last Seen and OS columns might be hidden if you view the Devices page in a narrow browser window.

2. To view detailed information about a device, click the device name. The device **Summary** tab shows detailed information about the device.

The **Device Information** area shows the following information about the device:

- **Status** – Status of the device. For possible values, see the previous step.
- **Last Seen** – Date and time when the agent was last in contact with the Management Console. The time is shown in your user's time zone set in the Management Console.
- **Availability** – Indicates whether each device is in contact with the Management Console. For possible values, see the previous step.
- **Hostname** – Name of the device. This is the Windows server name.
- **Site** – Site of the device.
- **Agent Version** – Version of the agent software installed on device.
- **Agent Upgrade Status** – Indicates whether the device's agent software is up to date or needs to be upgraded.
- **Keycode** – Keycode of the device's site. This keycode was entered when the Server Backup agent was installed on the device.

- **Server Backup Policy** – Server Backup policy assigned to the device.
- **Operating System** – Operating system of the device.

The **Server Backup** area shows the following information about the device's backups and recoveries:

- **Last Backup Attempt** – Time when the last backup started. The time is shown in your user's time zone set in the Management Console.
- **Last Backup Status** shows one of the following statuses:
 - **Completed Successfully** – The last backup on the device finished successfully.
 - **In Progress** – A backup is currently in progress on the device.
 - **Cancelled** – The last backup on the device was canceled by a user before it finished.
 - **Failed** – The last backup started but failed to complete.
- **Last Successful Backup** – Date and time when the last successful backup finished. The time is shown in your user's time zone set in the Management Console.
- **Entire Volume Recovery Status** shows one of the following statuses:
 - **No information to show** – A volume recovery is not in progress.
 - **View details** – A volume recovery is in progress or ran in the past two hours. Click **View details** to see the recovery process status. See *Recovering volumes* on page 52.
- **File and Folders Recovery Status** shows one of the following statuses:
 - **No information to show** – A file and folder recovery is in not in progress.
 - **View details** – A file and folder recovery is in progress or ran in the last two hours. Click **View details** to see the recovery process status. See *Recovering files and folders* on page 50.
- **DR Code** shows one of the following values:
 - **Not generated** – There is no active disaster recovery code for the device.
 - **Generated** – A disaster recovery code is active for the device.
- **DR Code Expiry** – Date and time when the disaster recovery code expires, if a disaster recovery code is active for the device. The time is shown in your user's time zone set in the Management Console.

3. To view detailed information about a backup or recovery, do one of the following:

- To view detailed information about the last backup, click **View event details** in the **Last Backup Status** section.
- To view information about another backup or recovery, click the **Event History** tab. To

view detailed information about a specific backup or recovery, click the activity in the **Event Type** column.

The **Event Details** window shows detailed information about the event, including the start and end date and time, status, and location of the log file on the device where the agent is installed. The Event Date and Time is shown in your user's time zone set in the Management Console. The Backup Start and End Times are specified in the time zone of the device where the agent is installed.

4. To view the progress of a backup that is running, click **View details** in the **Last Backup Status** section.

6.1 Running unscheduled backups

When the Server Backup agent is installed on a device, the agent backs up data automatically as specified by its storage location and policy.

You can also run a backup on demand at any time for an online device. You cannot run an unscheduled backup for a device that is offline, scheduled for deletion, expired, or has a backup in progress.


Note: If a backup is interrupted, data that was already backed up to the cloud will not be sent again. For example, if the connection between a server and AWS is disrupted during a large seed/full backup, the next backup does not send data that was already backed up to the cloud, saving time and bandwidth.

To run unscheduled backups:

1. In the navigation pane, go to **Server Backup > Devices**.
2. Click the name of a site that has one or more devices that you want to back up.
3. Do one of the following:
 - To back up one device, click the name of the device. The device **Summary** tab shows information about the device and its backups.
 - To back up one or more devices, select the check box for each device on the **Devices** page.
4. Click **Agent Commands** and then click **Run Backup**.

A confirmation message appears. If you are trying to run a backup for a device that is offline, scheduled for deletion, expired or has a backup in progress, a message indicates that a backup will not start for these devices.
5. (Optional) If you are troubleshooting issues, select **Run backup with verbose logging**.
6. Click **Send Command**.

If you are backing up one device, the **Backup Progress** box shows the backup progress.

If you are backing up more than one device, a Backup in Progress icon  appears for each device on the **Devices** page. To see the progress of a backup, click the device name. On the


device **Summary** tab, beside the Last Backup Status, click **View details**. The **Backup Progress** box appears.

7. (Optional) In the **Backup Progress** box, do one of the following:
 - To close the **Backup Progress** box without stopping the backup, click **Close**.
 - To stop the backup, click **Cancel**.

6.2 Monitoring or stopping a backup

You can view the progress of a backup and, if desired, stop the backup.

To monitor or stop a backup:

1. On the **Devices** page, click the name of the device that is being backed up. A Backup in Progress icon  appears beside each device that is being backed up.
2. On the device **Summary** tab, in the **Server Backup** area, click **View details**.

The **Backup Progress** box shows the backup progress.

3. Do one of the following:
 - To close the **Backup Progress** box without stopping the backup, click **Close**.
 - To stop the backup, click **Cancel**. In the confirmation box, click **Cancel Backup**. A message states that the cancellation request was sent. Another message appears when the backup is canceled. You can then click **View event details** to view information about the canceled backup.

Note: There can be a delay before the **Cancel** button is available in the **Backup Progress** box.

6.3 Changing an agent password

When you install an agent, you must specify a password for encrypting the agent data. You can change the password any time without reseeding the backup data.

If you change an agent password after the device is backed up, you can restore data from any recovery point using the new password; you do not need to remember the original password. Both new backups and previous backups for the device use the new password to restore.

You can only change an agent password for a device that is online.

IMPORTANT: The agent password is required for recovering the data, so be sure to keep it somewhere safe. The password is not maintained anywhere else. If you forget your password, you will not be able to recover your data or change the agent password.

To change an agent password:

1. In the navigation pane, go to **Server Backup > Devices**. The **Devices** page lists devices where the Server Backup agent is installed.
(Optional) To view devices in a particular site, click the site name in the **Sites** list.
2. Click the name of the device for which you want to change the agent password.
The status of the device must be **Online**, or you cannot change the password.
3. In the **Agent Commands** list, click **Update Password**.
4. In the **Enter Old Password** box, type the current password for the agent.
5. In the **Enter New Password** and **Confirm New Password** boxes, type the new password for the agent.
The password can have ASCII characters only, with no spaces or angled brackets < >. The following special characters are allowed: !"#%&'()*+,-./:;=?@[\]^_`{|}~
6. Click **Send Command**.

6.4 Deleting a device or canceling a deletion

You can delete a Server Backup device from the Management Console and delete its backups from cloud storage.


To protect against inadvertently deleting the wrong device data, a device is scheduled for deletion four days after you submit the deletion request. You can cancel the scheduled device deletion during this four-day period. While a device is scheduled for deletion, scheduled and on-demand backups do not run and you cannot restore the device data.

If you do not cancel a scheduled device deletion within the four-day period, the device is deleted from the Management Console and the device's backup data is deleted from storage. The agent can no longer contact the Management Console, but the agent software remains on the device. You can manually uninstall the agent from the device.

Note: After a device is deleted from the Management Console, there is sometimes a delay before its data is deleted from storage. Depending on the amount of data, it can take several days to delete the data. You cannot recover device data during this time.

To delete a device:

1. In the navigation pane, go to **Server Backup > Devices**.
2. Do one of the following:
 - To delete one device, click the name of the device that you want to delete. On the device details page, click **Agent Commands > Delete Device**.
 - To delete one or more devices in a site, click the site name. Select the check box for each device that you want to delete. Click **Agent Commands > Delete Device**.
3. In the **Agent Command: Delete Device** window, click **Send Command**.

The status of each device changes to **Scheduled for Deletion**. To see the date and time when a device and device data is scheduled for deletion, point to the question mark  beside the device's **Scheduled for Deletion** status.

To cancel a device deletion:

1. In the navigation pane, go to **Server Backup > Devices**.
2. Do one of the following:
 - To cancel the deletion of one device, click the name of a device that is scheduled for deletion. On the device details page, click **Cancel Device Deletion**.
 - To cancel the deletion of one or more devices in a site, click the site name. Select the check box for each device for which you want to cancel the scheduled deletion. Click **Agent Commands > Cancel Device Deletion**.
3. In the **Agent Command** box, click **Send Command**.

7 Monitoring Server Backup

You can monitor devices where Server Backup agents are installed, and monitor backups and recoveries using the following pages and tools:

- Dashboard. See *Monitoring Server Backup using the dashboard* below.
- Email notifications. See *Setting up email notifications* on the next page.

If you manage Server Backup customers using Secure Cloud, you can also view Server Backup information on the Secure Cloud Home page. For more information, see the Secure Cloud help and videos.

7.1 Monitoring Server Backup using the dashboard

You can monitor Server Backup devices, backups, and recoveries using the Management Console dashboard. Tiles on the dashboard show information about Server Backup agent installations, recoveries, and backups in the past 15 days, as well as the current status of devices where the Server Backup agent is installed.

You can navigate from tiles on the dashboard to reports with additional information.

To monitor devices using the dashboard:

1. In the navigation pane, click the **Dashboard** tab.

The dashboard shows tiles with information about your cybersecurity products.

2. View Server Backup information in the following tiles and navigate to related reports as required.

- **Successful Recoveries**. This tile shows the number of successful recoveries in the past 15 days, and a chart that shows the number of successful recoveries each day. To view the number of recoveries on a specific day, point to a bar in the chart. If you click the **Successful Recoveries** tile, you are redirected to the **Recovery History** report.
- **Server Backup Installs**. This tile shows the number of agents installed in the past 15 days, and a chart that shows the number of devices where a Server Backup agent was installed each day. To view the number of agents installed on a specific day, point to a bar in the chart. If you click the **Server Backup Installs** tile, you are redirected to the **Device Installs** report.
- **Backup Summary**. This tile shows the number of backups in the past 15 days and a line graph showing the number of backups and their statuses each day, including successful, failed, and canceled. To view backups on a specific day, point to the day in the bar chart. If you click the **Backup Summary** tile, you are redirected to the **Backup History** report.
- **Device Status**. This tile shows the most recently-received statuses of devices where Server Backup agents are installed. If you click the **Device Status** tile, you are redirected to the **Device Status** report.

When you click a tile and are redirected to a report, the report is filtered to show detailed information about data in the tile. You can change the data range and filters for the report. See *Viewing and exporting Server Backup reports* on page 47.

7.2 Setting up email notifications

To help you monitor Server Backup devices, backups and recoveries, you can set up email notifications for specific events. For example, you can set up notifications that are sent when a Server Backup agent is installed, an agent password is changed, or a backup or recovery runs. You can also delete email notifications.

You can also set up email notifications for other cybersecurity products in the Management Console. For more information, see the *Endpoint Protection Administration Guide*.

To set up email notifications:

1. In the navigation pane, click the **Notifications** tab.
2. Do one of the following:
 - To create a new notification, click **Add**.
 - To copy a notification, click **Copy** in the notification's **Actions** menu.
 - To edit a notification, click **Edit** in the notification's **Actions** menu.
3. In the **Name** box, enter a name for the notification.
4. In the **Email Recipients** box, enter up to 20 email addresses for sending the notification.

Note: You can enter any email addresses. The addresses do not have to be associated with console users.

5. In the **Event Type** list, choose the event for sending Server Backup email notifications:
 - **Device Install** to send notifications when an agent is installed on a device.
 - **Device Settings Change** to send notifications when the agent password on a device is changed. The agent password is used to encrypt and recover device data. For more information, see *Changing an agent password* on page 41.
 - **Device Backup** to send notifications when backups run.
 - **Device Deletion** to send notifications when devices are scheduled for deletion, devices are deleted, or scheduled deletions are canceled. For more information, see *Deleting a device or canceling a deletion* on page 42.
 - **Device Recovery** to send notifications when a recovery runs.
6. In the **Scope** list, do one of the following:
 - To send email notifications when the specified event occurs in any site in the console, click **Global**.

Note: **Global** is only available if you are signed in to the console as a Super Admin or parent admin.

- To send email notifications when the specified event occurs in a specific site, click the site name.
7. In the **Language** list, choose the language for the emails.
 8. Click **Save**.

To delete email notifications:

1. In the navigation pane, click the **Notifications** tab.
2. Find the notification that you want to delete. In the Actions menu for the email notification, click **Delete**.
3. In the confirmation message box, click **Delete**.

8 Viewing and exporting Server Backup reports

You can view reports with detailed information about Server Backup devices, backups, and recoveries. For a list of available reports, see *Server Backup reports* on the next page.


Each report includes a graph with summary information, and a table with detailed records. You can click points in the graph to see related records in the table. You can also click a device name in the table to navigate to detailed information about the device.

You can export data from some reports in .csv format. When you export data, a link to the report data file is sent to your sign-in email address.

To view and export Server Backup reports:

1. In the navigation pane, click **Reports**. On the **Reports** page, click the name of the Server Backup report that you want to view.

To find Server Backup reports in grid view , go to the Server Backup section of the page.

To find the reports in list view , sort the reports by product. You can also enter some or all of a report name in the **Search** box.

Note: You can also open a report by clicking a related tile on the dashboard. For more information, see *Monitoring Server Backup using the dashboard* on page 44.

2. Specify which data to show in the report by doing one or more of the following:
 - To only include records for a specific site, choose the site from the **Sites** list.
 - To change the date range of records in the report, click the date range box and do one of the following:
 - Click a time period from the list, such as **Last 30 Days** or **This Month**.
 - Click a start date and end date in the calendars, and then click **Apply**.

Note: The date range box is not applicable to all reports.

Note: Report data is available for the past year.

- To only include records with specific values, click **Filters** and then select the check box for each value you want to include in the report.

Note: The **Filters** button is not available for all reports.

3. To see the number of records associated with a point in the graph, point to the graph.

The number of records appears in a tooltip. In some reports, the number is divided into different categories, such as backup or recovery statuses.

4. To see the records that are associated with a point in a graph, click the point in the graph.
The table below the graph is filtered to show records associated with that point in the graph.

5. To export data from the report in .csv format, click **Export**.

A link to the data file is sent to your sign-in email address. Click the link in the email to download the report data file.

Note: Exporting is not available for all reports.

6. To view detailed information about a device in the report, click the device name in the report table.

You are redirected to detailed information about the device on the **Server Backup > Devices** page.

8.1 Server Backup reports

You can view the following Server Backup reports in the Management Console:

- **Backup History:** Shows backups that occurred during a specified time period. The report graph shows the number of backups with each status, including "Completed", "Failed", and "Canceled", over the time period. The report table provides detailed information about each backup, including the device name, backup date and time, status, and the amount of data backed up.
- **Device Deletion History:** Shows devices where deletion-related events occurred during a specified time period. Events include device deletions from the Management Console, scheduled deletions, and canceled deletions. The report table provides detailed information about each event, including the device name, the user who performed the action, and the date of the event.
- **Device Installs:** Shows Server Backup agent installations during a specified time period. The report table shows the name of each device where an agent was installed, the site name, and the date when it was installed.
- **Device Status:** Shows the most recent statuses reported by Server Backup devices. Statuses include "Protected", "Needs Attention", and "Scheduled for Deletion". The report table provides detailed information about each device, including its status, site name, and time of the status update.

Note: If you uninstall the Server Backup agent from a server and reinstall it on the same system with the same computer name, only the "new" agent status appears in the report. The original agent status will not be shown, even if the original agent is marked for deletion. Both the original agent and the new agent appear on the Devices page.

- **Recovery History:** Shows volume and file and folder recoveries that occurred during a specified time period. The report shows the status of each recovery, including "Completed", "Timed Out", and "Canceled". The report table provides detailed information about each recovery, including the device name, status, type ("Volume" or "File and Folder"), and date.

For information about viewing the reports and exporting report data, see *Viewing and exporting Server Backup reports* on page 47.

Note: Times in the reports are shown in your user's time zone set in the Management Console.

9 Recovering files and folders

To recover specific files and folders, you can mount volumes from a backup as temporary drives on the server that was backed up. You can then copy files and folders from the mounted drives to a permanent location. This recovery method is intended for recovering a limited number of files and folders. To recover entire volumes, see *Recovering volumes* on page 52.

You can only recover files and folders from devices that have been backed up and are online. You cannot recover files and folders from devices with the Pending, Scheduled for Deletion, or Expired status, or from devices that are offline.

When you recover files and folders from a backup, you must choose a recovery point. A recovery point is a backup that started on a specific day at a specific time. The time of each recovery point is shown in the real local time of the device where the agent is installed. Using the real local time ensures that recovery point times are always in chronological order, even if the system time changed on the device.

Note: If a device is not synchronized with a Network Time Protocol (NTP) server, the system time on the device can be different than the real local time.

To recover files and folders:

1. In the navigation pane, go to **Server Backup > Devices**.
2. Click the name of the device from which you want to recover files and folders.

Note: You cannot recover files and folders from devices with the Pending, Scheduled for Deletion, or Expired status, or from devices that are offline.

3. On the device details page, click **Agent Commands > Recover**.

Note: You can also start a recovery from the devices list. Select the check box for a device, and then click **Agent Commands > Recover**.

4. In the **Agent Command: Recover** wizard, on the **Password** page, type the agent encryption password in the **Enter Agent Password** box, and then click **Next**.

Note: If you enter an incorrect password five times, the device data is locked and no one can recover the device data for five minutes.

5. On the **Recovery Point** page, do the following:
 - a. In the calendar, click the day with the backup from which you want to recover files and folders.
 - b. In the **Recovery Point** list, select the check box for the time of the backup from which you want to recover files and folders.

The time of each recovery point is shown in the real local time of the device where the agent is installed.

- c. Click **Next**.
6. On the **Recovery Type** page, click **Recover Files and Folders**, and then click **Next**.
7. On the **Location** page, do the following:
 - a. In the **Mount Session Time Out** box, specify the number of minutes of inactivity on a mounted volume after which the volume will be automatically unmounted. Inactivity occurs when no files are being retrieved from the volume.
 - b. In the **Source Volume** column, select the check box for each volume in the backup from which you want to recover files and folders.
 - c. In the **Temporary Mount Volume** column, select the drive letter for mounting each volume from the backup.
 - d. Click **Send Command**.

The **Recovery Progress** box shows the status of mounting each volume on the server.

Note: If the Recovery Progress box closes, you can reopen it by clicking **View details** beside **File and Folders Recovery Status** on the **Summary** tab for the device.

8. When each volume is mounted, go to the server where you are recovering files and folders, and manually copy files and folders from the temporarily-mounted drives to drives on the server.
9. (Optional) When you finish copying files and folders from each mounted drive to the server, click **Dismount All**. The status of volume mount is then **Completed** in the **Recovery Progress** box.

If you do not dismount the volumes, the volumes automatically dismount from the server after the time specified in the **Mount Session Time Out** box in Step 7 above. The status of each volume mount is then **Timed Out** in the **Recovery Progress** box.

10 Recovering volumes

You can recover volumes on a server by mounting them on the server where they were backed up and copying them to a permanent drive on the server.

You can only recover volumes from devices that have been backed up and are online. You cannot recover volumes from devices with the Pending, Scheduled for Deletion, or Expired status, or from devices that are offline.

When you recover volumes from a backup, you must choose a recovery point. A recovery point is a backup that started on a specific day at a specific time. The time of each recovery point is shown in the real local time of the device where the agent is installed. Using the real local time ensures that recovery point times are always in chronological order, even if the system time changed on the device.

Note: If a device is not synchronized with a Network Time Protocol (NTP) server, the system time on the device can be different than the real local time.

To recover volumes:

1. In the navigation pane, go to **Server Backup > Devices**.
2. Click the name of the device from which you want to recover one or more volumes.

Note: You cannot recover volumes from devices with the Pending, Scheduled for Deletion, or Expired status, or from devices that are offline.

3. On the device details page, click **Agent Commands > Recover**.

Note: You can also start a recovery from the devices list. Select the check box for a device, and then click **Agent Commands > Recover**.

4. In the **Agent Command: Recover** wizard, on the **Password** page, type the agent encryption password in the **Enter Agent Password** box, and then click **Next**.

Note: If you enter an incorrect password five times, the device data is locked and no one can recover from device data for five minutes.

5. On the **Recovery Point** page, do the following:
 - a. In the calendar, click the day with the backup from which you want to recover volumes.
 - b. In the **Recovery Point** list, select the check box for the time of the backup from which you want to recover volumes.

The time of each recovery point is shown in the real local time of the device where the agent is installed.

- c. Click **Next**.
6. On the **Recovery Type** page, click **Recover Entire Volume**, and then click **Next**.

7. On the **Location** page, do the following:

- a. In the **Volume to Recover** column, select the check box for each volume that you want to restore from the backup.
- b. In the **Target Volume Destination** column, select the drive letter for restoring each volume from the backup.
- c. Click **Send Command**.

The **Recovery Progress** box shows the status of the volume recovery. A progress bar appears while the recovery is in progress.

To cancel the recovery of a volume, click **Cancel** in the volume row.

Note: There can be a delay before **Cancel** appears in the **Recovery Progress** box.

11 Recovering servers after a disaster

If a Windows server is lost, you can recover the entire server, including its operating system and system state, from a backup. You can recover:

- One server to physical hardware or a virtual machine. See *Recovering a Windows server to hardware or to a virtual machine* below.
- One or more servers to Amazon Elastic Compute Cloud (Amazon EC2) in the AWS account where your backups are stored. During the recovery process, an EC2 instance is created for each recovered server. See *Recovering Windows servers to the AWS cloud* on page 58.

If you need to recover a server to physical hardware but new hardware is not yet available, you can temporarily recover the server to Amazon EC2. Backups will continue while the server runs in EC2. Once the physical hardware is available, you can recover the server from a backup in EC2 to the physical hardware.

You can also test a server recovery. In a test recovery, the Windows server is recovered but does not replace the original device in the Management Console. In a full recovery, the recovered server replaces the original device in the Management Console and backups continue automatically on the new server.

11.1 Recovering a Windows server to hardware or to a virtual machine

You can recover a Windows server to physical hardware or to an existing virtual machine. The recovered server automatically replaces the original device in the Management Console and backups continue on the new server.

You can also test a Windows server recovery. In a test recovery, the server is recovered but does not replace the original device in the Management Console.

To recover a Windows server to hardware or to an existing virtual machine, do the following:

- a. Download the BMR (Bare Metal Restore) Media Creator from the Management Console, and use it to create recovery media. Recovery media is used to boot destination machines and recover Windows servers. See *Downloading the BMR Media Creator* on the next page and *Creating recovery media* on the next page. You can use the same recovery media to recover multiple servers, so you do not need to create recovery media every time you recover a server.
- b. Obtain a disaster recovery code. See *Obtaining a disaster recovery code* on page 57.
- c. Use the recovery media to boot the machine where you want to recover the server, and recover the Windows server. You must enter the disaster recovery code during this process. See *Recovering a Windows server* on page 66.
- d. Repair the recovered server's operating system and drivers. See *Repairing a recovered server* on page 85.

11.1.1 Downloading the BMR Media Creator

Note: If you already have a copy of the BMR Media Creator, you do not need to download it again. Go to *Creating recovery media* below.

To download the BMR Media Creator:

1. In the Management Console, go to **Server Backup > Devices** in the navigation pane.
2. Click the name of a device with the **Protected** or **Needs Attention** status. On the device details page, click **Disaster Recovery**.
3. On the **Disaster Recovery** page, click **Recover to hardware or virtual environment**, and then click **Next**.

Note: The **Recover to hardware or virtual environment** option is only available if at least one scheduled backup has run for the device. The option is not available if only the initial backup after installation and unscheduled backups have run.

4. If a message says that a previously-generated Disaster Recovery code is active, click **Cancel** so you do not interfere with the other recovery. Restart this procedure, and select a different device in Step 2.
5. Click **Download BMR Media Creator**.

11.1.2 Creating recovery media

You must create recovery media using the BMR Media Creator before you can recover a Windows server from a backup. Recovery media is a USB flash drive or other bootable device with a BMR Agent ISO image file, and is used to boot destination machines and recover Windows servers.

Note: You do not need to create recovery media every time you recover a server. You can use the same recovery media to recover multiple Windows servers. However, you must create separate recovery media to restore servers with different Windows Server versions: one for servers with Windows Server 2022 and later versions, and one for servers with Windows Server 2019 and earlier versions.

The Windows Assessment and Deployment Kit (Windows ADK) and the Windows Preinstallation Environment (Windows PE) must be installed on the system where you run the BMR Media Creator. You can download Windows ADK and Windows PE from Microsoft and install them before running the BMR Media Creator or when you run the BMR Media Creator. For required Windows ADK and Windows PE versions, see *BMR Media Creator supported platforms, requirements and known issues* on page 92. For more information about Windows ADK and Windows PE, see documentation from Microsoft.

To create recovery media:

1. If the BMR Media Creator is not installed on the machine where you want to create recovery media, do the following:

- a. Double-click the BMR Media Creator installation kit that was downloaded in *Downloading the BMR Media Creator* on the previous page.
 - b. If a message states that the BMR Media Creator requires one or more items to be installed, click **Install**.
 - c. On the **Welcome** page, click **Next**.
 - d. On the **Ready to Install the Program** page, click **Install**.
 - e. When the installation is completed, click **Finish**.
2. Start the BMR Media Creator.
3. On the **Creating recovery media** page, click the operating system of the devices that you want to recover:
 - **Windows Server 2022 and later**
 - **Windows Server 2019 and earlier**
4. Click **Continue**.
5. If the **Install Windows Assessment and Deployment Kit for Windows** page appears, you must install Windows ADK before you can create recovery media. Click **Install** to download the Windows ADK installer from Microsoft, and then install Windows ADK. When the installation is finished, click **Continue**.

For more information about Windows ADK, see documentation from Microsoft.

6. If the **Install WinPE add-on for Windows Assessment and Deployment Kit for Windows** page appears, you must install WinPE before you can create recovery media. Click **Install** to download the WinPE installer from Microsoft, and then install WinPE. When the installation is finished, click **Continue**.

For more information about WinPE, see documentation from Microsoft.

7. On the **Select Your Media Device** page, do one of the following:
 - To create recovery media on a USB flash drive, select **USB Flash Drive**, and choose a flash drive from the list. To add a flash drive to the list, insert the flash drive into a USB port, and click **Refresh** when it is ready.

The flash drive storage capacity must be at least 500 MB.
 - To create a BMR Agent ISO image file, select **ISO Image**, and specify a location for saving the file.

After creating a BMR Agent ISO image file, you must burn it to a bootable CD or DVD, attach the ISO file to a Hyper-V or VMware virtual machine, or set up a PXE boot server before you can use it as recovery media.
8. (Optional) To add drivers for specialized hardware, click **Add** on the **Build Bootable Media Image** page. In the **Browse for Folder** dialog box, browse to the location of driver (.inf) files, and then click **OK**.
9. Click **Continue**.
10. When a message states that your recovery media is ready, click **Close**.

11.1.3 Obtaining a disaster recovery code

A disaster recovery code is required for recovering a server using recovery media. The recovery code (also known as a disaster recovery or DR code) can only be used once and is valid for one week.

To obtain a disaster recovery code:

1. In the navigation pane, go to **Server Backup > Devices**.
2. (Optional) Click the name of the site with the device that you want to recover.
3. Click the name of the device that you want to recover. On the device details page, click **Disaster Recovery**.

Note: You can only recover a server with the **Protected** or **Needs Attention** status. You cannot recover a server that has the **Pending** or **Scheduled for Deletion** status.

4. On the **Disaster Recovery** page, click **Recover to hardware or virtual environment**, and then click **Next**.

Note: You can only recover to hardware or to a virtual machine if at least one scheduled backup has run for the device. The **Recover to hardware or virtual environment** option is not available if only the initial backup after installation and unscheduled backups have run.

5. If a message says that a previously-generated Disaster Recovery code is active, do one of the following:
 - To cancel the current recovery, click **Cancel**.
 - To continue the current recovery and cancel the other recovery that is in progress, click **Next**.
6. Do one of the following:
 - To recover the server, select **Recover server after a disaster**.
 - To test the server recovery, select **Test the disaster recovery process**. In a test recovery, the server is recovered but does not replace the original device in the Management Console.
7. Click **Generate Code**.

Note: You can also download the BMR Media Creator from this page if you have not yet created recovery media. See *Downloading the BMR Media Creator* on page 55 and *Creating recovery media* on page 55.

8. On the **Recovery Code** page, click **Copy** to copy the recovery code. Keep the recovery code somewhere safe. You need to enter the code to recover the server, and cannot view it in the Management Console after you close this page.

The recovery code can only be used once and is valid for one week. The expiry date and

time of the DR code appears on the **Summary** tab of the server's device details page.

9. Click **Close**.

You can then use the recovery media and disaster recovery code to recover the server to destination hardware or a virtual machine. For detailed instructions, see *Recovering a Windows server* on page 66.

11.2 Recovering Windows servers to the AWS cloud

You can recover one or more Windows servers to Amazon Elastic Compute Cloud (Amazon EC2) in the AWS account where your backups are stored. During the recovery process, an EC2 instance is created for each recovered server. The recovered servers automatically replace the original devices in the Management Console and backups continue on the new servers.

You can also test Windows server recoveries. In test recoveries, servers are recovered but do not replace the original devices in the Management Console.

After recovering a server to an EC2 instance, remote desktop will be enabled on the server and the firewall will allow remote desktop connections to the server.

To recover one or more Windows Servers to Amazon EC2, do the following:

- a. In the Management Console, start the disaster recovery. Select an EC2 instance type for each recovered server, and download your Disaster Recovery package. See *Starting a recovery to the AWS cloud* on the next page.

The Disaster Recovery package is a .zip file that includes a Disaster Recovery User Guide (DRRunbook.html), a CloudFormation template for creating EC2 instances and resources, a setup.ps1 script for orchestrating the creation of required resources in your AWS account, and a finalize.ps1 script for ensuring that recovered servers can boot properly.

- b. Follow the instructions in the Disaster Recovery User Guide to install prerequisites, create one or more EC2 instances and required resources, connect to the EC2 instances, and recover each server.

To create EC2 instances and required resources, you must configure the AWS CLI with an IAM user's access key and secret access key. The IAM user must be in the AWS account where your backups are stored and must have the permissions described in *AWS IAM role for recovering servers to the AWS cloud* on page 61.

When your original environment is operational and you no longer need the recovered servers in your AWS account, remove the AWS resources that were created during the disaster recovery. Leaving these resources in place can result in unnecessary AWS charges and may cause you to reach AWS service limits. For more information, see *Decommissioning AWS resources after recovery* on page 65.

11.2.1 Starting a recovery to the AWS cloud

To start a recovery to the AWS cloud:

1. In the navigation pane, go to **Server Backup > Devices**.
2. Do one of the following:
 - To recover one server, click the name of the device that you want to recover. On the device details page, click **Disaster Recovery**.
 - To recover one or more servers, click the name of the site with the device or devices that you want to recover. Select the check box for each device that you want to recover. Click **Disaster Recovery**. If a message states that unsupported devices are selected, read which devices cannot be recovered, and click **Next**.

Note: You can select a maximum of 25 devices to recover at one time.

Note: You cannot recover devices with the Pending, Scheduled for Deletion, or Expired status.

3. On the **Disaster Recovery** page, click **Recover to the cloud**, and then click **Next**.
4. Read the overview of the disaster recovery process, and then click **Next**.
5. Do one of the following:
 - To recover one or more servers, click **Recover one or more servers after a disaster**.
 - To test the server recovery, click **Test the disaster recovery process**. In a test recovery, servers are recovered but do not replace the original devices in the Management Console.

6. Click **Next**.

The **Disaster Recovery** page shows the AWS region where the server or servers will be recovered and a **Device Selection** area where you can choose an EC2 instance type for each recovered server. Selected devices that cannot be recovered appear in the **Device Selection** area, but you cannot select EC2 instances for them.

Note: Servers are recovered to the AWS region where the site's backups are stored.

7. For each server that you are recovering, select an EC2 instance type by doing the following in the **Instance Type** column:
 - a. Filter the list of EC2 instance types in the **Select an instance** list by doing the following:
 - In the **CPUs** list, select the approximate number of CPUs for the EC2 instance.

Note: The number of CPUs and amount of RAM in the original server appear in the **Device Name** column under the server name.

- In the **RAM** list, select the approximate amount of memory (in GB) for the EC2 instance.
- To restrict the list of EC2 instances to cost-effective instances that are suitable for most applications, make sure that the **Show Preferred Instances** check box is selected. When this check box is selected, the **Select an instance** list only includes EC2 instances in the M (General purpose), C (Compute optimized), T (Burstable performance), and R (Memory optimized) series. For more information, see *Amazon EC2 instance types* documentation on the Amazon Web Services (AWS) website.

The **Select an instance** list includes EC2 instance types that are available in the site's AWS region and match the filter criteria.

Note: When restoring to the AWS cloud, you can only restore to an EC2 instance with the UEFI boot mode.

- b. In the **Select an instance** list, choose the EC2 instance type for the recovered server.
8. Click **Next**.
 9. Click **Download All Documents**.

A Disaster Recovery package (CloudDisasterRecoveryArtifacts.zip) file is downloaded that includes a Disaster Recovery User Guide (DRRunbook.html), a CloudFormation template for creating EC2 instances and resources, and scripts for creating and finalizing your servers. Recovery codes (also known as a disaster recovery or DR codes) in the package can only be used once and are valid for one week. The expiry date and time of the DR code for a server appears on the **Summary** tab of its device details page.

Note: If you download a new Disaster Recovery package for the same servers, it will replace the previous one. You can only use the most recently-downloaded Disaster Recovery package to restore your servers.

10. Click **Finish**.
11. In the confirmation message box, click **Close**.

You can then follow the instructions in the Disaster Recovery User Guide (DRRunbook.html) and use the provided scripts in the Disaster Recovery package to:

- i. Create an EC2 instance for each server you are recovering and create required files and resources.
- ii. Connect to your servers in AWS.

IMPORTANT: If you are recovering a server to an EC2 instance and the original server is still accessible in your network, you might have trouble connecting to the EC2 instance. To prevent this issue, turn off the original server or disconnect it from the network.

- iii. Recover data to each EC2 instance using the BMR Agent. The BMR Agent is pre-installed on each EC2 instance. For detailed instructions, see *Recovering a Windows*

server on page 66.

- iv. Finalize the recovery to ensure that servers can boot properly.

If you recovered one or more servers (rather than testing the recovery process), the recovered servers replace the original servers in the Management Console and backups continue automatically.

11.2.2 AWS IAM role for recovering servers to the AWS cloud

When recovering servers to Amazon EC2 in the AWS account where your backups are stored, you must configure the AWS CLI with an IAM user's access key and secret access key. The IAM user must have permissions for the following AWS services:

- **EC2.** The user must be able to:
 - Run and manage instances, and create and manage volumes.
 - Create and manage security groups, virtual private clouds (VPCs), subnets, route tables, DHCP options, NAT gateways, and VPNs.
 - Describe other resources, including regions, availability zones, IP addresses, account attributes, and network information.
- **Certificate Manager.** The user must be able to import and list certificates.
- **CloudFormation.** The user must be able to create and manage stacks and stack resources.
- **Identity and Access Management (IAM).** The user must be able to create and manage roles, policies, and instance profiles.
- **S3.** The user must be able to add objects to S3 buckets.

The following sample policy shows permissions for recovering servers to Amazon EC2.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Allow",
      "Action": [
        "ec2:TerminateInstances",
        "ec2:StartInstances",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceAttribute",
```

```
"ec2:DescribeInstanceCreditSpecifications",
"ec2:CreateTags",
"ec2:AllocateAddress",
"ec2:ReleaseAddress",
"ec2:CreateVolume",
"ec2:DeleteVolume",
"ec2:AttachVolume",
"ec2:DetachVolume",
"ec2:DescribeVolumes",
"ec2:CreateSecurityGroup",
"ec2:DeleteSecurityGroup",
"ec2:DescribeSecurityGroups",
"ec2:AuthorizeSecurityGroupIngress",
"ec2:CreateVpc",
"ec2:DeleteVpc",
"ec2:DescribeVpcs",
"ec2:DescribeVpcAttribute",
"ec2:ModifyVpcAttribute",
"ec2:DescribeVpcBlockPublicAccessOptions",
"ec2:DescribeVpcEndpoints",
"ec2:DescribeVpcEndpointServiceConfigurations",
"ec2:DescribeVpcPeeringConnections",
"ec2:AttachInternetGateway",
"ec2:DetachInternetGateway",
"ec2:CreateInternetGateway",
"ec2:DeleteInternetGateway",
"ec2:DescribeInternetGateways",
"ec2:CreateSubnet",
"ec2:DeleteSubnet",
"ec2:ModifySubnetAttribute",
"ec2:DescribeSubnets",
"ec2:CreateRouteTable",
"ec2:DeleteRouteTable",
```

```
"ec2:CreateRoute",
"ec2:DeleteRoute",
"ec2:AssociateRouteTable",
"ec2:DisassociateRouteTable",
"ec2:DescribeRouteTables",
"ec2:CreateDhcpOptions",
"ec2:DeleteDhcpOptions",
"ec2:AssociateDhcpOptions",
"ec2:DescribeDhcpOptions",
"ec2:CreateNatGateway",
"ec2:DeleteNatGateway",
"ec2:DescribeNatGateways",
"ec2:CreateClientVpnEndpoint",
"ec2:DeleteClientVpnEndpoint",
"ec2:AssociateClientVpnTargetNetwork",
"ec2:DisassociateClientVpnTargetNetwork",
"ec2:AuthorizeClientVpnIngress",
"ec2:RevokeClientVpnIngress",
"ec2:ExportClientVpnClientConfiguration",
"ec2:DescribeClientVpnEndpoints",
"ec2:DescribeClientVpnAuthorizationRules",
"ec2:DescribeClientVpnTargetNetworks",
"ec2:DescribeVpnConnections",
"ec2:DescribeVpnGateways",
"ec2:DescribeCustomerGateways",
"ec2:DescribeRegions",
"ec2:DescribeAvailabilityZones",
"ec2:DescribeAddresses",
"ec2:DescribeAccountAttributes",
"ec2:DescribeNetworkAcls",
"ec2:DescribeNetworkInterfaces",
"ec2:DescribeInstanceConnectEndpoints",
"ec2:DescribeEgressOnlyInternetGateways",
```

```
"ec2:AssociateClientVpnTargetNetwork",
"ec2:RunInstances",
"ec2:RevokeSecurityGroupIngress",
"ec2:AuthorizeSecurityGroupEgress",
"ec2:AuthorizeSecurityGroupIngress",
"ec2:RevokeSecurityGroupEgress",
"ec2:RevokeSecurityGroupIngress",
"acm:ImportCertificate",
"acm:ListCertificates",
"cloudformation:CreateStack",
"cloudformation>DeleteStack",
"cloudformation:UpdateStack",
"cloudformation:DescribeStacks",
"cloudformation:ListStacks",
"cloudformation:DescribeStackEvents",
"cloudformation:ListStackResources",
"cloudformation:CreateUploadBucket",
"cloudformation:CreateChangeSet",
"iam:CreateRole",
"iam>DeleteRole",
"iam:PassRole",
"iam:AttachRolePolicy",
"iam:DetachRolePolicy",
"iam:CreateInstanceProfile",
"iam:AddRoleToInstanceProfile",
"iam:RemoveRoleFromInstanceProfile",
"iam>DeleteInstanceProfile",
"iam:CreatePolicy",
"iam:CreatePolicyVersion",
"iam>DeletePolicyVersion",
"iam:GetPolicy",
"iam:GetPolicyVersion",
"iam:ListRoles",
```



```
        "iam:PutRolePolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:CreateServiceLinkedRole",
        "s3:PutObject"
    ],
    "Resource": ["*"]
}
]
```

11.2.3 Decommissioning AWS resources after recovery

After your original systems are restored and your production environment is stable, you should remove the AWS resources that were created during the disaster recovery process. Leaving these resources in place can result in unnecessary AWS charges and may cause you to reach AWS service limits.

IMPORTANT: Do not complete this cleanup until AWS failover is no longer needed. This prevents accidental removal of resources required for ongoing recovery.

Before you begin

Before you decommission AWS resources, make sure that your original environment is fully operational and that you no longer need the AWS recovery environment. Perform this cleanup only after you have confirmed that failure to AWS is no longer required.

To decommission AWS resources after recovery:

1. Review resources created by the CloudFormation stack.

When you recover Windows servers to the AWS cloud, the disaster recovery process creates an AWS CloudFormation stack that provisions multiple resources. To see which resources were created:

- a. Sign in to the AWS Management Console.
- b. Navigate to the CloudFormation console.
- c. Click the stack that was created for disaster recovery
- d. Click the **Resources** tab.

This tab lists all resources created by the stack, including their logical and physical IDs and the AWS service they belong to

- e. Review the list of resources carefully.

IMPORTANT: If you do not have permission to delete certain resources (for example, IAM roles, security groups, or VPC components), note them down. You will need to follow your company's process to remove these resources later.

2. Delete the CloudFormation stack.

- a. In the CloudFormation console, select the stack that you want to delete.
- b. Click **Delete**, and confirm the deletion.

The stack will attempt to remove all resources it created.

Note: Any resources you do not have permission to delete will remain in your account. These must be removed manually or by an administrator.

3. Remove residual resources.

If resources remain after the stack deletion, follow your company's policy to remove them. This ensures that you do not incur additional charges or reach AWS resource limits.

11.3 Recovering a Windows server

You can use recovery media to recover each Windows server. Recovery media is a USB flash drive or other bootable device with a BMR Agent ISO image file, and is used to boot destination machines and recover Windows servers.

If you are recovering a server to hardware or to a virtual machine, you must create recovery media as described in *Recovering a Windows server to hardware or to a virtual machine* on page 54. You can use the recovery media to boot the destination server and recover the machine. For destination server requirements, see *Choosing a recovery server* on page 69.

If you are recovering one or more Windows servers to the AWS cloud, recovery media is pre-installed on each EC2 instance created during the process described in *Recovering Windows servers to the AWS cloud* on page 58. After recovering a server to an EC2 instance, remote desktop will be enabled on the server and the firewall will allow remote desktop connections to the server.

Using recovery media, you can only restore volumes to basic disks. However, you can convert basic disks to dynamic disks after starting a recovered system. For more information, see *Recovering dynamic disks and spanned volumes* on page 83.

When device installation restrictions in a system's group policy could prevent a recovered system from starting successfully, the BMR Agent tries to change the device installation restrictions. You can change the device installation restrictions back after starting the recovered system. For more information, see *Recovering servers with device installation restrictions* on page 82.

Note: If you are recovering a server (not testing the disaster recovery process), make sure that the original server is offline. Otherwise, backups might not continue after the recovery.

To recover a Windows server:

1. Choose a recovery (destination) server where the source (backed up) server will be restored. For recovery server requirements, see *Choosing a recovery server* on page 69.

2. Boot the recovery server from the recovery media.

If the BMR Agent is on a bootable USB flash drive, CD or DVD, the device should be the first option in the boot order of the firmware. If another bootable device is listed before the recovery media, the BMR Agent might not launch automatically.

If the BMR Agent ISO file is on a PXE server, the PXE option must be enabled in the firmware and the DHCP server must be set up in the network where the system resides.

3. On the **Server Backup** page, specify the time zone and keyboard, and then click **Next**.

This time zone is used for showing available recovery points (i.e., backup start times) during the recovery. The recovered server will have the time zone of the system that was backed up.

4. On the **Server Backup - Public Cloud: BMR Agent** page, click the **Recover my system** button.

The BMR Agent wizard lists steps in the recovery process.

5. Read the steps, and then click **Next**.

6. On the **Enter DR code and Password** page, do the following:

- a. In the **Disaster Recovery Code** box, enter the disaster recovery (DR) code. If you are recovering a Windows server to hardware or to a virtual machine, the code was provided in the Management Console. If you are recovering a server to the AWS cloud, the code appears in the Disaster Recovery User Guide (DRRunbook.html), which is part of the Disaster Recovery package downloaded from the Management Console.

IMPORTANT: Enter the disaster recovery (DR) code exactly as it appeared in the Management Console or Disaster Recovery User Guide. The code is case-sensitive and must include all characters, including dashes.

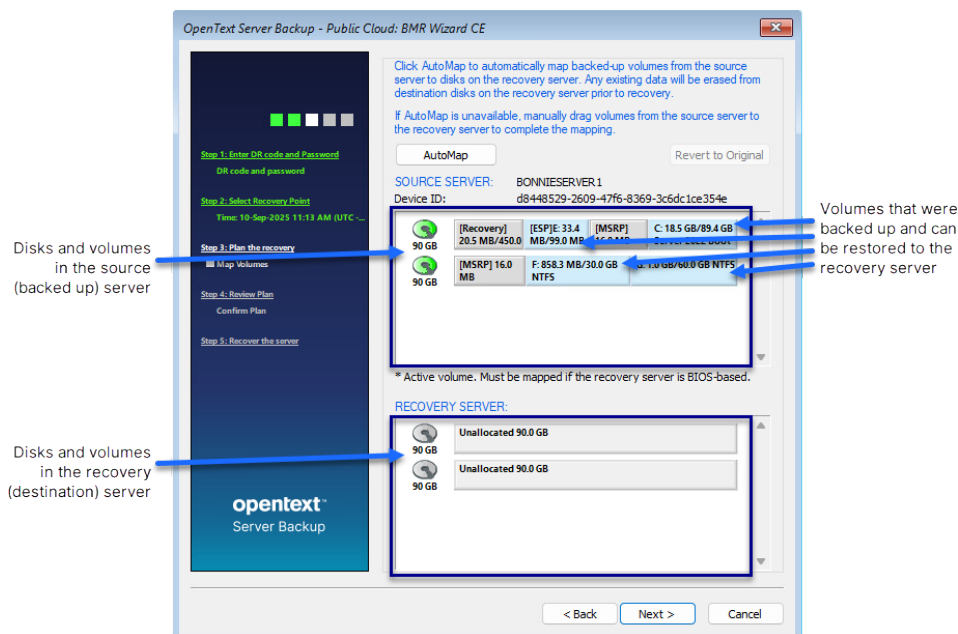
- b. In the **Agent Password** box, enter the password used to encrypt the agent's data.

- c. Click **Next**.

7. On the **Select Recovery Point** page, click the recovery point from which you want to restore, and then click **Next**.

Each recovery point is the start date and time of a backup, shown in the time zone selected in Step 3.

The **Plan the recovery** page appears. This page shows disks and volumes in the source (backed up) server and in the recovery (destination) server. Blue rectangles in the Source Server section represent volumes that were backed up and can be restored. For more information about items on the page, see *Source and recovery server icons* on page 74.



Using this page, you can create a recovery plan. A recovery plan shows which volumes from the source server to restore to disks on the recovery server. Blue rectangles in the Recovery Server section represent volumes that will be restored.

Note: If disks are missing from the recovery server, you might need to add drivers for a RAID controller or other disk device.

8. Do one of the following:

- To automatically create a recovery plan, click **AutoMap**.

Note: The **AutoMap** button does not appear unless the source server and recovery server meet the requirements described in *Automatically mapping drives in a recovery* on page 70. If the button does not appear, you must map volumes manually.

- To map volumes manually from the source server to disks in the recovery server, drag volumes from the Source Server area to the Recovery Server area. For more information, see *Manually mapping drives in a recovery* on page 71.

(Optional) To remove volumes from the Recovery Server area and start mapping volumes again, click **Revert to Original**.

9. Click **Next**.

The **Review Plan** page lists changes that will be made in the destination server if you run the recovery.

10. Review the recovery plan. Do one of the following:

- To recover the source server as shown in the recovery plan, select **Click here to confirm the recovery plan**, and then click **Next**. The recovery begins. The BMR

wizard shows the recovery progress.

Note: Incorrect drive letters might be temporarily assigned until you restart the recovered server. For example, the C: drive might be assigned to the F: drive. When you restart the recovered server, the correct drive letters will be assigned.

- To change the recovery plan, click **Back**, and then repeat Steps 8 and 9.

11. When a message box states that the restore was completed successfully, click **OK**.
12. On the **Recovery progress** page, click **Next**.
13. On the **Congratulations** page, click **Next**.

A repair process begins and the **Repair Wizard** page appears. See *Repairing a recovered server* on page 85.

14. To start the recovered server, select **Reboot the system**. Click **Finish**.

Note: A recovery must finish within 72 hours or it will fail. This time limit is from the Windows Preinstallation Environment (Windows PE), which is used during the recovery.

Note: After you recover a system with more than one disk, you might need to bring the disks online using the Disk Management utility or diskpart command interpreter in Windows.

11.3.1 Choosing a recovery server

Before recovering a Windows server, you must choose a recovery server where the server will be restored.

The recovery server can be the machine where the server was backed up, or can be a different physical or virtual machine. If you restore a server to the machine where it was backed up, files will be restored to their state when the server was backed up.

When recovering a Windows server, the recovery server:

- Must have 64-bit hardware. The BMR Agent can only restore a system to 64-bit hardware.
- Can be a physical or virtual machine (VM). You can restore a backup of a physical computer to a physical or virtual machine, and can restore a backup of a virtual computer to a physical or virtual machine.

When restoring a computer to a VM, ensure that the VM configuration is compatible with the computer that is being recovered.

- Can use UEFI or BIOS. You can restore a backup of a BIOS-based computer to a BIOS or UEFI machine. You can restore a backup of a UEFI-based computer to a UEFI machine, but cannot restore a backup of a UEFI-based computer to a BIOS machine. For more information, see *Recovering UEFI-based systems* on page 80 and *Recovering BIOS-based systems* on page 81.

- Can have an operating system and files, or can be in a bare metal state. If you restore to a machine that has an operating system and data, the existing files will be overwritten.
- Can have similar hardware to the source server, or can have dissimilar hardware.

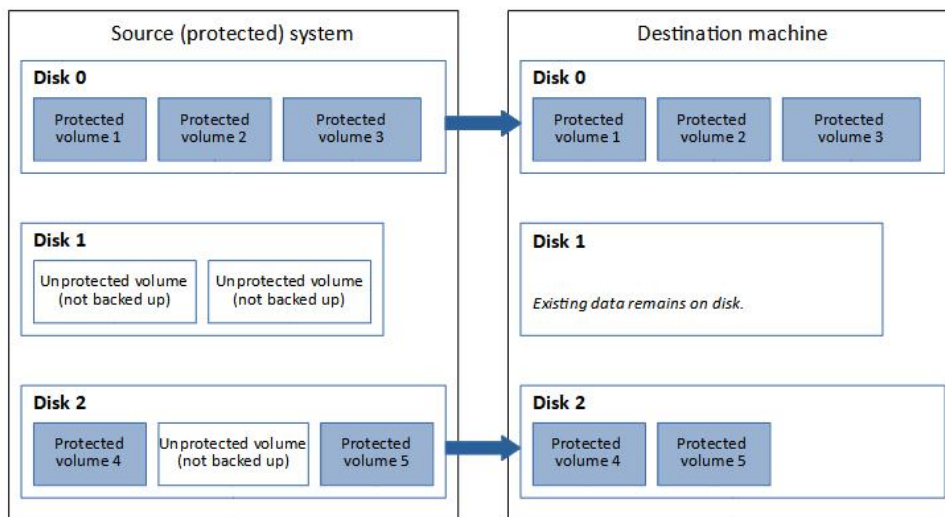
If the recovery server hardware supports the operating system of the source server you are restoring, you should be able to restore even if, for example, the disks are different. You might not be able to restore if the recovery server hardware is incompatible with the source server operating system.

Some non-Intel or non-AMD processors, such as Itanium, might not restore to Intel/AMD processors.

11.3.2 Automatically mapping drives in a recovery

If the **AutoMap** button is available during a system recovery, you can automatically map volumes from a backup to a recovery server. This simplifies the restore process, as you do not have to manually drag volumes from the source server to the recovery server in the BMR Agent wizard.

If you click the **AutoMap** button during a restore, the BMR Agent automatically maps all protected volumes from the source (protected) server to corresponding disks on the recovery (destination) server, and clears any existing data from the destination disks. Data is not cleared from disks that are not destinations in the recovery. For example, as shown in the following diagram, volumes from Disk 0 and Disk 2 in a source server are mapped to Disk 0 and Disk 2 in the destination server, and existing data remains on Disk 1 in the destination server.



The AutoMap feature is available when the source and destination servers meet the following requirements:

- The source and destination servers use the same firmware: either UEFI or BIOS.
- The source (protected) server has a maximum of four disks. None of the protected disks can be dynamic disks.
- The destination server has a maximum of four disks.

- The destination server has the same number or more disks than in the source system. For example, if volumes are backed up on the first three disks in a source server, the destination server must have three or more disks. If volumes are backed up on the first, third and fourth disk in the source server, the destination server must have four disks.
- Disks where volumes will be restored on the destination server are the same size or larger than the corresponding disks on the source server.

If you are restoring a BIOS-based computer, the Automap feature is not available if an MBR volume from the source system would be mapped to a disk larger than 2 TB on the destination machine.

Note: These conditions are usually met if you restore a server to the same hardware where it was backed up.

11.3.3 Manually mapping drives in a recovery

After creating recovery media, you can recover a Windows server from a backup to a destination server. The destination server can be a physical or virtual machine where the system was backed up or a different machine. For more information, see *BMR Agent supported platforms, requirements and known issues* on page 94.

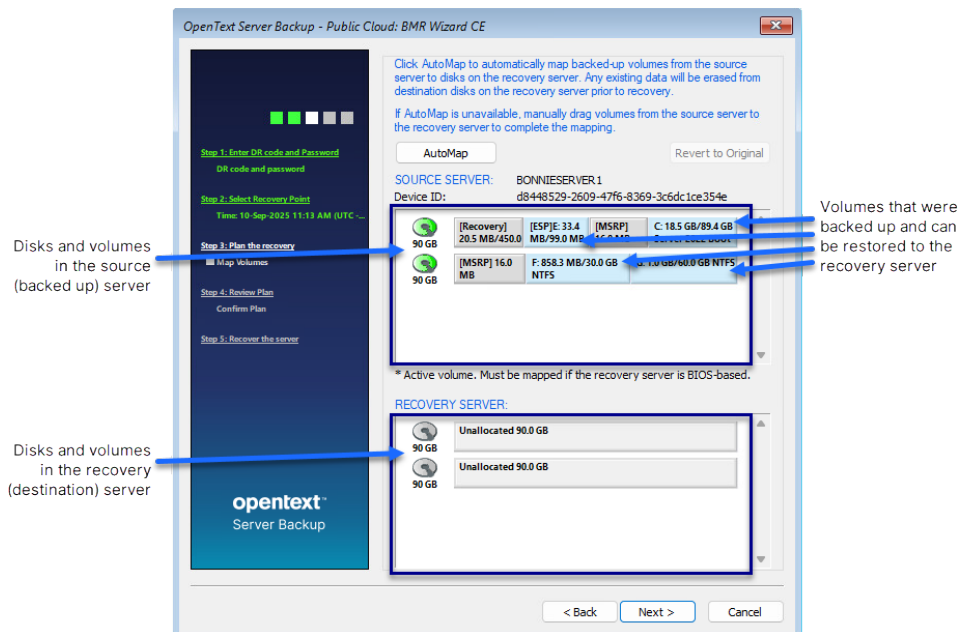
Using recovery media, you can only restore volumes to basic disks. However, you can convert basic disks to dynamic disks after starting a recovered system. For more information, see *Recovering dynamic disks and spanned volumes* on page 83.

When device installation restrictions in a system's group policy could prevent a recovered system from starting successfully, the BMR Agent tries to change the device installation restrictions. You can change the device installation restrictions back after starting the recovered system. For more information, see *Recovering servers with device installation restrictions* on page 82.

Note: If you are restoring a system to a different destination machine (i.e., not the machine where it was backed up), make sure that the original machine is offline. This will help avoid IP address and name conflicts after the restore.

To map drives manually during a recovery:

1. Start the recovery as described in *Recovering a Windows server* on page 66. Complete steps in the BMR Agent wizard until you see the **Plan the recovery** page. This page shows disks and volumes in the source (backed up) server and in the recovery (destination) server. Blue rectangles in the Source Server section represent volumes that were backed up and can be restored. For more information about items on the page, see *Source and recovery server icons* on page 74.



Using this page, you can create a recovery plan. A recovery plan shows which volumes from the source server to restore to the recovery server. Blue rectangles in the Recovery Server section represent volumes that will be restored.

Note: If disks are missing from the recovery server, you might need to add drivers for a RAID controller or other disk device.

2. (Optional) To make room for volumes that you want to recover by deleting a volume from the recovery server, right-click the volume in the **Recovery Server** area, and click **Delete Volume**.

Note: You can delete an MSRP volume using this method if it is the last partition remaining on a disk. To delete an MSRP volume that is not the last partition remaining on a disk, right-click the disk icon and change the disk format.

3. (Optional) To view a volume label in a tooltip, point to the volume.
4. Do one or more of the following until the **Recovery Server** area shows the volumes that you want to restore to the recovery server:
 - To convert a disk in the recovery server to GPT or MBR, right-click the disk icon and choose **Convert to GPT disk** or **Convert to MBR disk**.
 - If the source server has an "ESP" volume:
 - i. Drag the ESP volume from the source server to the start of a GPT-formatted disk in the recovery server.

If a message states that an EFI partition can only be restored to a UEFI system, you are trying to restore the system to a BIOS machine. You can only restore a UEFI-based system to a UEFI destination machine.

- ii. Drag the "Boot" volume from the source server to the right of the ESP volume in the recovery server.
- iii. Drag other volumes that you want to restore, if any, from the source system to the recovery server.

A system with an ESP volume is UEFI-based. For more information, see *Recovering UEFI-based systems* on page 80.

- If the source server has a "System" volume:
 - i. Drag the "Boot" volume from the source server to the start of a GPT-formatted disk in the recovery server.

If an ESP volume is created automatically in the recovery server, you do not need to restore the System volume.
 - ii. If an ESP volume is not created automatically, drag the System volume to the right of the Boot volume.

If a message states that the volume is an OEM volume, delete the Boot volume from the recovery server disk. Drag the System volume to the start of the recovery server disk, and then drag the Boot volume to the right of the System volume. For more information, see *Recovering systems with OEM partitions* on page 82.
 - iii. Drag other volumes that you want to restore, if any, from the source server to the recovery server.

A system with a "System" volume is BIOS-based. For more information, see *Recovering BIOS-based systems* on page 81.

- To remove volumes from the Recovery Server area and start mapping volumes again, click **Revert to Original**.

5. Click **Next**.

The **Review Plan** page lists changes that will be made in the recovery server if you run the recovery.

6. Review the recovery plan. Do one of the following:

- To recover the source server as shown in the recovery plan, select **Click here to confirm the recovery plan**, and then click **Next**. The recovery begins. The BMR wizard shows the recovery progress.

Note: Incorrect drive letters might not be temporarily assigned until you start the recovered server. For example, the C: drive might be assigned to the F: drive. When you restart the recovered server, the correct drive letters will be assigned.

- To change the recovery plan, click **Back**, and then repeat Steps 8 and 9.

7. When a message box states that the restore was completed successfully, click **OK**.

8. On the **Recovery progress** page, click **Next**.

9. On the **Congratulations** page, click **Next**.

A repair process begins and the **Repair Wizard** page appears. See *Repairing a recovered server* on page 85.

10. To start the recovered server, select **Reboot the system**. Click **Finish**.

Note: A recovery must finish within 72 hours or it will fail. This time limit is from the Windows Preinstallation Environment (Windows PE), which is used during the recovery.


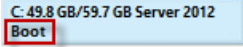
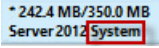

Note: After you recover a system with more than one disk, you might need to bring the disks online using the Disk Management utility or diskpart command interpreter in Windows.

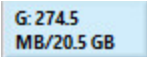
11.3.4 Source and recovery server icons

As described in *Recovering a Windows server* on page 66, on the **Plan the recovery** page of the BMR Agent wizard, you can map drives from the source (backed up) server to the recovery (destination) server. Icons on the page represent volumes and disks in the servers, as described in the following tables.

Volumes that were backed up (Blue rectangles)


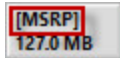
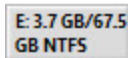
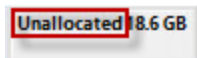

Blue rectangles represent volumes that were backed up on the source server and can be recovered.

Item	Example	Description
ESP/EFI partition		An Extensible Firmware Interface (EFI) System Partition. A UEFI-based system must have an EFI system partition or the system will not boot up. See <i>Recovering UEFI-based systems</i> on page 80.
Boot volume		A boot volume. A BIOS-based system must have a boot volume or the system will not boot up. See <i>Recovering BIOS-based systems</i> on page 81.
System volume		A system volume. A BIOS-based system must have a system volume or it will not boot up. See <i>Recovering BIOS-based systems</i> on page 81. A volume with the "System" label can also be an OEM partition. See <i>Recovering systems with OEM partitions</i> on page 82.
System and Boot volume		A volume that is both a system and boot volume. See <i>Recovering BIOS-based systems</i> on page 81.

Item	Example	Description
Optional volume		Volume that was backed up and can be restored, but is not required for the destination machine to boot up.




Volumes that were not backed up (Gray rectangles)

Gray rectangles represent volumes that were not backed up on the source server and cannot be recovered.

Item	Example	Description
Recovery volume		A recovery volume that contains system files, drivers and factory default setup information. Recovery volumes are not backed up.
MSR partition		Microsoft Reserved (MSR) partition. An MSR partition is disk space reserved for Windows use on a GPT disk. If one is required in the destination machine, it is created automatically.
Volume		In a source system, a volume that was not backed up. In a destination machine, an existing volume on the disk. You can delete, change or overwrite an existing volume.
Unallocated space		Unallocated space on a disk.
Free space		Free space on a disk.

Disk icons

An icon appears for each disk in the source server and destination server. The icon color represents the disk format.

Item	Example	Description
GPT-formatted disk		A green disk icon represents a GPT-formatted disk. If you drag a volume to an uninitialized disk on a UEFI destination machine, the disk type automatically changes to GPT.
MBR-formatted disk		A blue disk icon represents an MBR-formatted disk.
Uninitialized disk		A gray disk icon represents an uninitialized disk.

11.3.5 Setting up a network connection for the BMR Agent

To run a restore, the BMR Agent requires a network connection. The network connection is normally set up automatically. However, if DHCP is not configured on the network or you want to use a static IP address, you can set up the connection manually.

Note: This process sets up a network connection for the BMR Agent, not for the restored system. You can configure networking for the restored system after you start it.

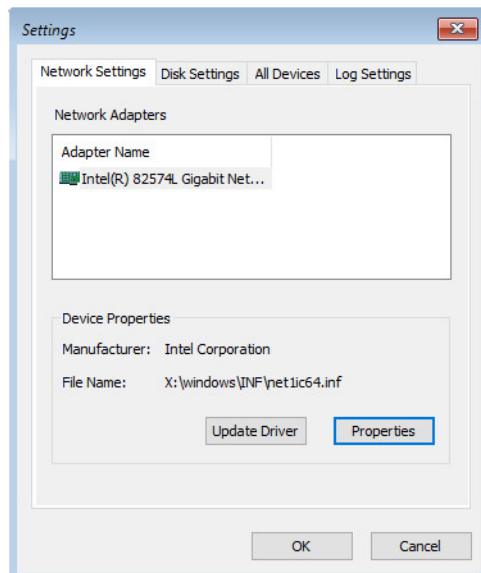
To set up a network connection for the BMR Agent:

1. In the BMR Agent wizard, do one of the following:
 - To set up a default network connection, click **Settings** on the **Server Backup - Public Cloud: BMR Agent** page.



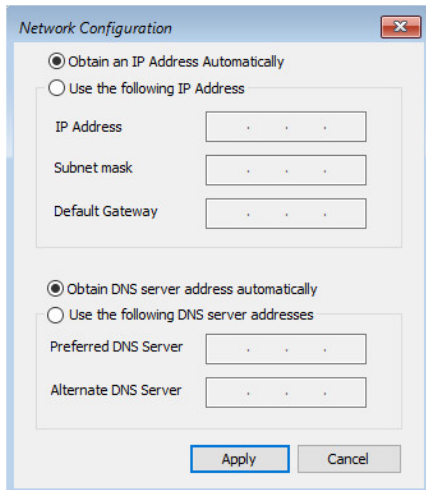
- To set up a network connection for a specific restore, click **Recovery Settings** on the **Enter DR code and Password** page.

The **Settings** dialog box shows recognized network adapters in the destination machine. The **Device Properties** area shows driver information for the selected adapter.



2. To install or update the driver for a network adapter, select the adapter, and then click **Install** or **Update Driver**. In the **Install Driver** box, do one of the following:

- To install the driver from a local disk, select **Local Disk**. Browse to the .inf file location, or enter the path to the driver manually.
 - To install the driver from a network share, select **Network Share**, and enter the path to the .inf file. You cannot browse to a network share.
3. Select the network adapter to use for the network connection.
 4. Click **Properties**. If a driver is installed for the adapter, a LAN is connected, and a port is enabled, the **Network Configuration** dialog box appears.



5. In the **Network Configuration** dialog box, select **Use the following IP Address**.
6. Enter the IP address, subnet mask, and default gateway for the network adapter.
7. If you have DHCP and want to access other systems using domain names instead of IP addresses, select **Use the following DNS server addresses**. In the **Preferred DNS Server** field, enter the primary DNS IP address for the network adapter. You can also provide an IP address for an alternate DNS server.
8. Click **Apply**.

11.3.6 Installing or updating device drivers

The BMR Agent includes commonly-used recovery-critical drivers. You can install other drivers for destination machine devices. For example, if you cannot see all available storage devices in the destination machine when restoring a system, you might need to add a driver for a RAID controller or other disk device. You can also update existing drivers.

To install or update a device driver:

1. In the BMR Agent wizard, do one of the following:
 - To change the default network settings, click **Settings** on the **Server Backup Public Cloud - BMR Agent** page.



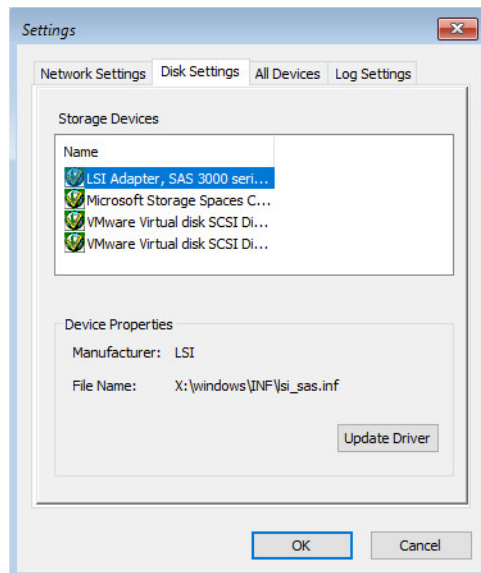
- To change network settings for a specific restore, click **Restore Settings** on the **Choose Backup Location** page.

The **Settings** dialog box shows recognized network adapters in the destination machine. The **Device Properties** area provides driver information for the selected adapter.

2. In the **Settings** dialog box, do one of the following:

- To install or update a network adapter driver, click the **Network Settings** tab.
- To install or update a storage device driver, click the **Disk Settings** tab.
- To install or update another device (e.g., PCI device) driver, click the **All Devices** tab.

The tab lists devices in the destination machine.



3. Select the device for the driver installation or update.

If there is no driver for the device, the **Install** button appears. If there is a driver, the **Update Driver** button appears.

4. Click **Install** or **Update Driver**. In the driver dialog box, do one of the following:

- To install the driver from a local disk, select **Local Disk**. You can then browse to the .inf file location, or enter the path to the driver manually, and click **OK**.
- To install the driver from a network share, select **Network Share**. You can then enter the path to the .inf file manually, and click **OK**. You cannot browse to a network share.

5. Click **OK**.

11.3.7 Configuring recovery log settings

You can configure the following settings for BMR Agent recovery logs:

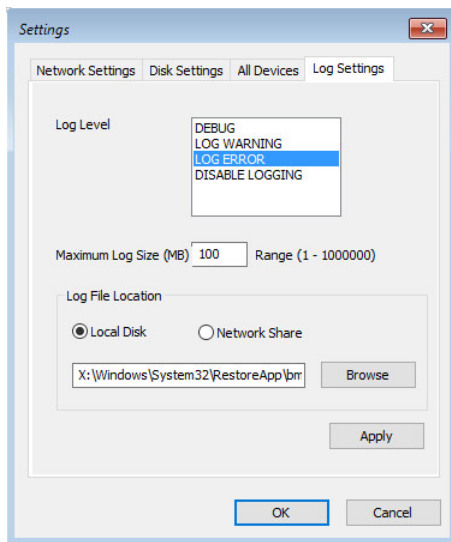
- Level of detail. You can include error messages only, warning and error messages, or all messages in the logs. You can also disable logging.
- Maximum log file size. When the maximum log file size is reached, the log starts overwriting the file from the beginning. By default, the maximum log file size is 100 MB.
- Log file location. By default, the log file is saved on the X: RAM drive, which is lost after reboots. We recommend saving logs on a separate device.

To configure recovery log settings:

1. On the **Server Backup - Public Cloud: BMR Agent** page, click **Settings**.



2. In the **Settings** dialog box, click the **Log Settings** tab.



3. In the **Log Level** list, do one of the following:
 - To record all messages in the log, select **Debug**.
 - To record warning and error messages, select **Log Warning**.
 - To only record error messages, select **Log Error**.
 - To not generate a log, select **Disable Logging**.
4. To change the maximum log file size, enter the size in MB in the **Maximum Log Size** box.

5. To change the log file location, do one of the following:
 - To specify a log file location on a local disk, select **Local Disk**. Browse to the location, or enter the path manually.
 - To specify a log file location on a network share, select **Network Share**, and enter the path manually. You cannot browse to a network share.
6. Click **Apply**.
7. Click **OK**.

11.3.8 Running Windows utilities from a command prompt

You can open a command prompt from the BMR Agent and run Windows utilities that are available in the Windows Preinstallation Environment (WinPE). For example, you could open a command prompt and use ping to check for network connectivity.

To run Windows utilities from a command prompt:

1. On the Server Backup - Public Cloud: BMR Agent page, click **Command Prompt**.



The command prompt window opens.

2. Run Windows utilities from the command prompt.

11.3.9 System-specific recovery information

This section provides information about restoring specific types of Windows systems, including:

- *Recovering UEFI-based systems* below
- *Recovering BIOS-based systems* on the next page
- *Recovering systems with OEM partitions* on page 82
- *Recovering servers with device installation restrictions* on page 82
- *Recovering dynamic disks and spanned volumes* on page 83

11.3.9.1 Recovering UEFI-based systems

If a source (backed up) server on the **Plan the recovery** page includes a partition labeled “ESP”, the system is UEFI-based. An ESP (EFI system partition) is required for a recovered UEFI system to boot into Windows.



You can only recover a UEFI-based system to a UEFI recovery (destination) server. You cannot restore a UEFI-based system to a BIOS recovery server.

Restore the ESP partition from the source system to a GPT-formatted disk in the destination machine. If you drag a volume to an uninitialized disk on a UEFI system, the disk type automatically changes to GPT.

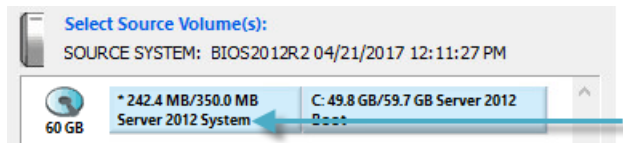
If an ESP volume already exists in the recovery server, the ESP partition from the protected machine should overwrite the existing ESP partition. You can also delete an existing ESP partition if, for example, it is too small to overwrite.

The order of partitions on the GPT disk should be: ESP, OEM (if any) and MSR followed by primary data partition(s). Partition order rules are enforced during a restore.

If required, an MSR (Microsoft Reserved) partition is automatically created on the destination machine during a UEFI system restore.

11.3.9.2 Recovering BIOS-based systems

If a protected (source) system on the **Plan the recovery** page includes a partition labeled “System”, the system is BIOS-based.



You can restore a BIOS-based system to a UEFI or BIOS destination machine.

Recovering a BIOS-based system to a UEFI destination machine

If you drag the Boot volume from a protected BIOS-based system to a UEFI destination machine, an ESP volume is generated automatically in the destination machine. An ESP (EFI system partition) is required for a UEFI system to boot into Windows.

The ESP partition must be on a GPT-formatted disk in the destination machine. If you drag a volume to an uninitialized disk on a UEFI system, the disk type automatically changes to GPT.

The order of partitions on the GPT disk should be: ESP, OEM (if any) and MSR followed by primary data partition(s). Partition order rules are enforced during a restore.

If required, an MSR (Microsoft Reserved) partition is automatically created in the destination machine.

You do not have to restore the System volume from a protected BIOS-based system to a UEFI destination machine.

When restoring a volume from a BIOS-based system to a UEFI destination machine, there might not be enough space, even if the destination disk is the same size. This problem can occur because an uninitialized UEFI disk defaults to GPT format and additional space is required for a GPT partition table. To prevent this problem, choose a larger destination volume or convert the volume to MBR format.

Recovering a BIOS-based system to a BIOS destination machine

To restore a BIOS-based system to a BIOS destination machine, you must restore both the System volume and the Boot volume from the source to the destination machine. The destination disk must use MBR formatting. A BIOS-based system can have GPT-formatted disks, but cannot boot from a GPT disk.

An active partition is required for booting. The active partition is marked with an asterisk (*).

To avoid losing disk space, initialize all disks larger than 2TB as GPT format. MBR partitioning does not allow to use disk space beyond 2TB.

If the destination machine does not boot after the restore, you may need to go into the BIOS and select the disk for booting. Dragging the System/Active volume to the first disk in the destination machine usually avoids this problem.

11.3.9.3 Recovering systems with OEM partitions

You can recover a BIOS-based system with an Original Equipment Manufacturer (OEM) partition to a BIOS or UEFI destination machine.

Note: A “System” label appears on an OEM partition on the Select Source and Destination Volumes page in the restore wizard.

When restoring a protected (source) system with an OEM partition to a BIOS destination machine, the OEM partition must be restored or the system will not boot up. The OEM partition must be restored to the start of a destination machine disk.

When restoring a protected (source) system with an OEM partition to a UEFI destination machine, the OEM volume is not required for booting and does not have to be restored.

If you restore a system with an OEM operating system license to dissimilar hardware, the system might boot but you will not be able to log in to the system without activating Windows. This occurs because OEM licenses are not transferable. When the restore process finishes, contact Microsoft to activate the Windows license.

11.3.9.4 Recovering servers with device installation restrictions

When device installation restrictions in a system’s group policy could prevent a recovered server from starting successfully, the BMR Agent tries to change the device installation restrictions during a recovery.

You can change the device installation restrictions back after starting the recovered server.

To change device installation restrictions on a Windows server, do the following:

1. Start the recovered server.
2. Install required drivers.
3. Using the Registry Editor, import the HKEY_LOCAL_MACHINE_SYSTEM_DriverDatabase_Policies_Restrictions.reg file from the root of the Windows directory drive

(usually drive C) into HKEY_LOCAL_MACHINE\SYSTEM\DriverDatabase\Policies\Restrictions.

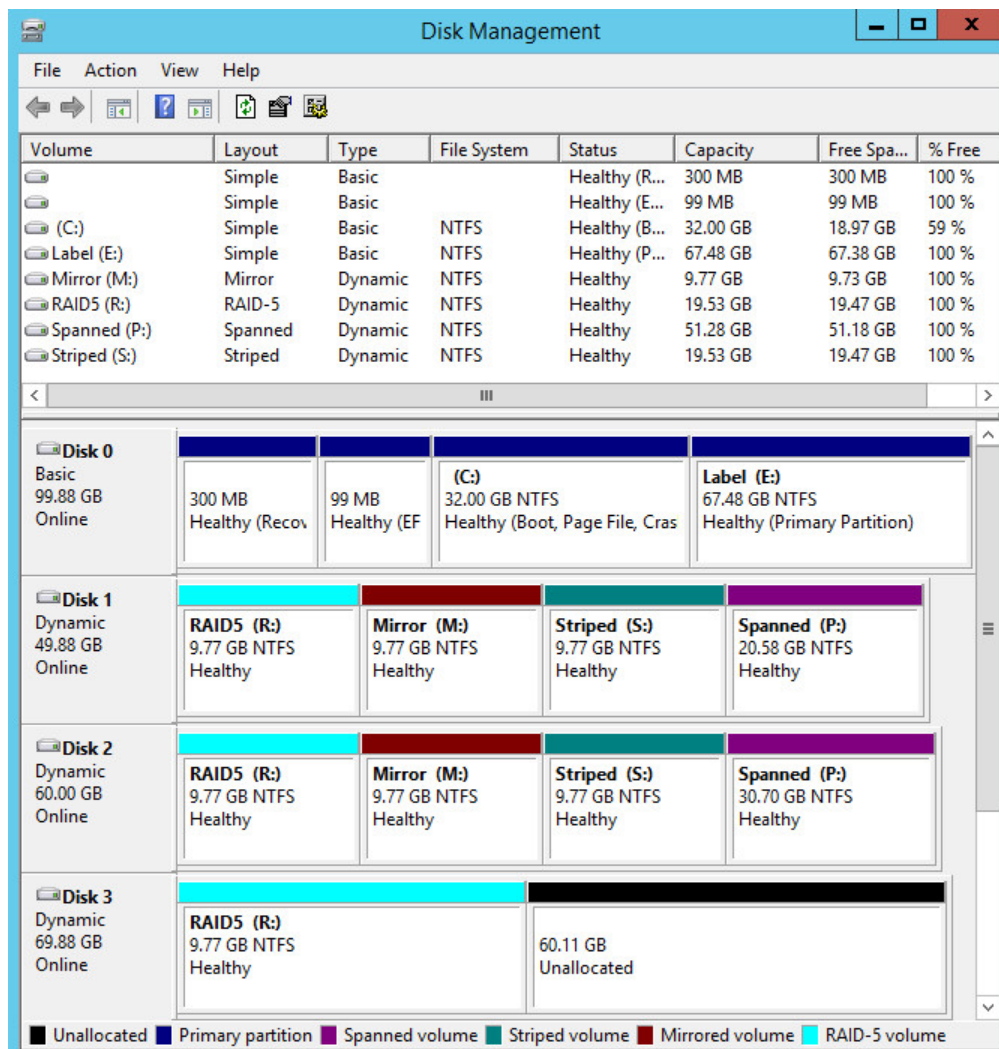
4. Using the Group Policy Editor, apply a change to a setting in Local Computer Policy\Computer Configuration\Administrative Templates\System\Device Installation\Device Installation Restrictions. The group policy settings will then be applied to the computer.

11.3.9.5 Recovering dynamic disks and spanned volumes

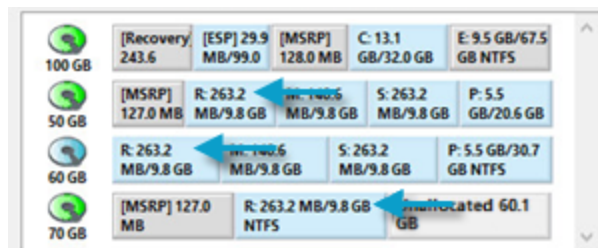
The BMR Agent can only restore volumes to basic disks. It cannot create dynamic disks, and cannot restore volumes to dynamic disks on destination machines. You can convert basic disks to dynamic disks after starting a restored system.

Dynamic disks do not appear to be dynamic on the **Plan the recovery** page of the Recovery wizard. When a volume in a source system spans dynamic disks, each portion of the spanned volume appears as a separate volume with the same drive letter. When a recovery server disk has dynamic partitions, one large volume appears for all dynamic partitions on the disk.

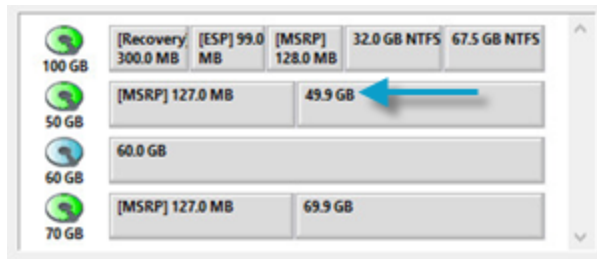
As an example, consider the system shown in the following Disk Management screen. This system has three dynamic disks (Disks 1, 2 and 3) and four volumes (R, M, S and P) that span disks.



When this system is the source server, each portion of a spanned volume appears as a separate volume with the same drive letter in the BMR Agent restore wizard. For example, the R spanned volume is shown as three separate R volumes.

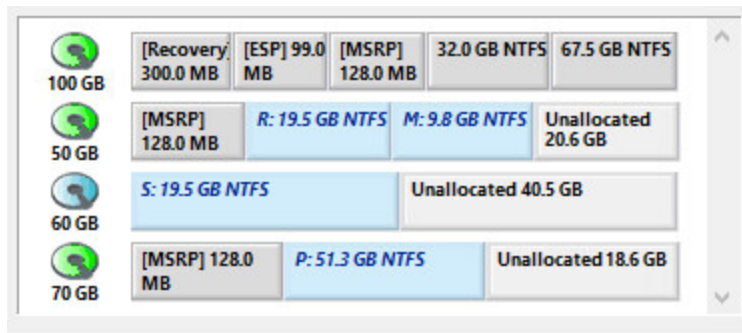


When this system is the recovery server, all dynamic partitions on a disk appear as one large volume in the BMR Agent Recovery wizard. For example, a 49.9 GB volume represents the portions of volumes R, M, S and P on Disk 1. You must delete this volume before you can restore data to the disk. Similarly, you must delete the 60.0 GB and 69.9 GB partitions before you can restore data to them.



When you restore a spanned volume to a recovery server, one basic volume is created for the contents of the entire spanned volume. The volume contains as much space as the original volume, unless a volume was only partially full and can fit in the recovery server. Volumes can only be restored as simple volumes, not spanned, RAID5, mirrored or striped.

The following screenshot and table show how volumes from the sample system are restored:



Volume	Original	Restored
P	Spanned volume with two parts: 20.6 GB and 30.7 GB	One 51.3 GB volume (20.6 GB + 30.7 GB)
S	Striped volume with two 9.8 GB parts	One 19.5 GB volume (approx. 2 * 9.8 GB)
M	Mirrored volume with two 9.8 GB parts. Second part for mirroring only.	One 9.8 GB volume
R	RAID5 volume. Three portions; 9.8 GB each. 2/3 of the RAID volume was used for data. The rest was used for parity.	One 19.5 GB volume (approx. 2/3 * (3 * 9.8 GB))

11.4 Repairing a recovered server

If you restore a system to a destination machine with different hardware, the restored system might not be able to boot. Drivers might be missing for boot-critical devices, and the Hardware Abstraction Layer (HAL) and kernel might not be optimal for the destination machine. You can repair boot-critical devices and perform HAL and kernel repairs using the BMR Agent.

Some drivers, such as network drivers, are not necessary for booting a system. After starting a recovered server, Windows can update drivers for devices that are not boot-critical.

Windows Server can repair drivers at boot if the drivers are provided with Windows.

To repair a recovered server:

1. If the BMR Agent detects that system repairs are necessary after a recovery, the repair wizard starts automatically at the end of the recovery.

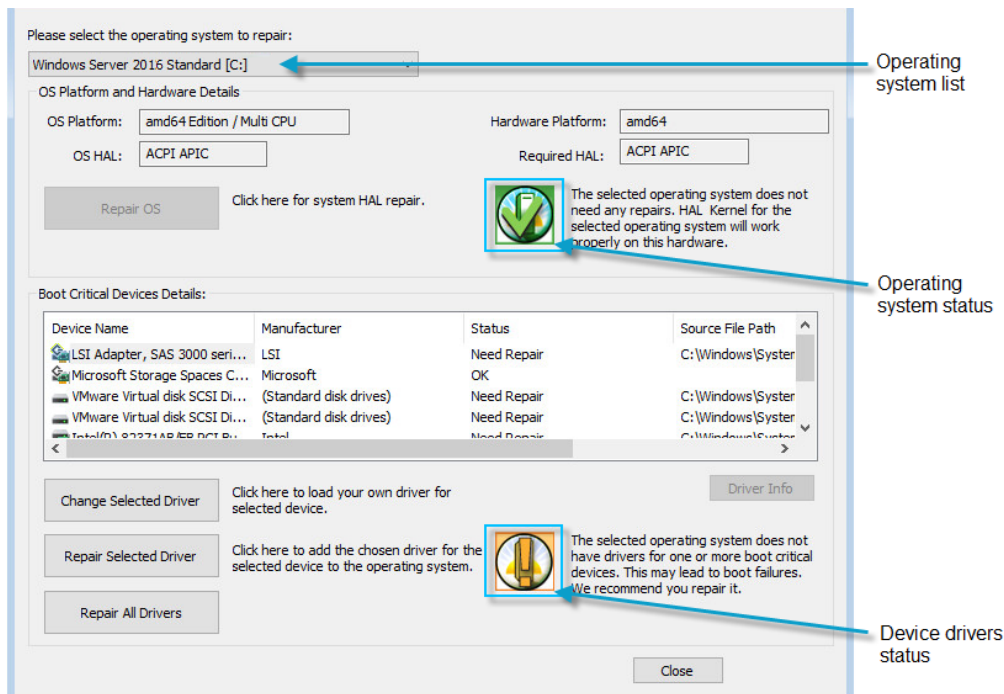
To start the repair wizard manually, click **Repair My System** on the **Server Backup -**





Public Cloud: BMR Agent page.

2. In the operating system list, select the operating system to repair.

The Repair wizard shows information about the operating system, hardware, and boot-critical devices. Status icons appear for the operating system and device drivers. For more information, see *Items in the Repair wizard* on the next page.



3. If a yellow operating system status icon  appears in the **OS Platform and Hardware Details** area, the operating system needs to be repaired. Click **Repair OS**.

4. If a yellow status icon  appears in the **Boot Critical Devices Details** area, at least one boot-critical driver needs repair. Do one or more of the following:
 - To repair drivers for all boot-critical devices that need repair, click **Repair All Drivers**.
 - To repair the driver for one boot-critical device that needs repair, click the device name and then click **Repair Selected Driver**.

If the BMR Agent cannot automatically repair the driver, a **Browse for Folder** dialog box appears. If you added the driver when you created recovery media for restoring to hardware or to a virtual machine (see *Recovering a Windows server to hardware or to a virtual machine* on page 54), you can find the driver (.inf) files in the Boot drive (usually X:\) in \Windows\System32\RestoreApp.

- To install a specific driver for a device, click the device name and then click **Change Selected Driver**. In the **Browse for Folder** dialog box, select the folder that contains the .inf file. If the BMR Agent cannot find a matching .inf file in the selected folder, a message appears.

Note: If the BMR Agent does not find the best driver for a device, it might use a more generic driver. Ideally, provide the latest driver (from the vendor) for your specific hardware.

- Click **Reboot** or **Shutdown**.




The **Reboot** button appears if you recovered the server to physical hardware or to a virtual machine. The **Shutdown** button appears if you recovered one or more servers to EC2. You must finalize recovered servers in EC2 before you can reboot them, as described in the Disaster Recovery User Guide downloaded when you started the recovery. See *AWS IAM role for recovering servers to the AWS cloud* on page 61.

- In the confirmation message box, click **Yes**.

11.4.1 Items in the Repair wizard



As described in *Repairing a recovered server* on page 85, the Repair wizard shows status icons for the operating system and boot-critical device drivers. The following tables describe possible icons and statuses.

OS Platform and Hardware status icons

Icon	Description
	Repair is not required. The HAL or kernel does not need to be adjusted for the current hardware.
	Repair is required. The operating system might not be able to boot with the current HAL. This can occur, for example, if you restore a single-CPU operating system to hardware with multiple CPUs or cores. In this instance, you can repair the operating system so that it uses all CPUs.
	Repair is not possible. The selected operating system is not compatible with the current hardware. For example, you cannot restore a non-ACPI operating system to ACPI-compatible hardware.

Boot Critical Devices status icons

Icon	Description
------	-------------

	Device drivers are OK. The selected operating system does not need new drivers for boot-critical devices.
	At least one device driver needs repair. The Status column for each device indicates whether its driver is OK or needs repair.

11.5 Recovering Active Directory servers: Enabling AD authentication for recovered servers via AWS VPN

This section describes how to allow Active Directory (AD) users to connect to servers recovered in an AWS private network through a VPN connection. The process involves:

- Creating an AWS AD Connector. See *Setting up the AWS AD Connector* below.
- Configuring an AWS Client VPN Endpoint using AD-based authentication. See *Configuring the AWS Client VPN Endpoint with AD Authentication* on the next page.

This section provides high-level information. For detailed information and procedures, see the *AWS AD Connector Guide* and *AWS Client VPN Guide* in AWS documentation.

Note: Refer to AWS pricing documentation for cost details.

11.5.1 Prerequisites

- AD Domain Controllers have been recovered and are operational.
- Networking and security groups allow required ports for AD communication.

11.5.2 Setting up the AWS AD Connector

1. In the AWS Management Console, go to the AWS Directory Service console.
2. Create an AD Connector.
3. Select the VPC and private subnet where the connector will reside.
4. Enter the following information:
 - Directory DNS name – For example, the name could be: corp.example.com
 - NetBIOS name – For example, the name could be: CORP
 - Service account credentials – The account must have permissions to read users and groups, and join computers to the domain.
 - DNS IP addresses of your AD domain controllers.
5. Ensure that the AD Connector status changes to Active.

Required Ports

For the AD Connector to redirect directory requests to your AD domain controllers, ensure that the AD Server's security group allows inbound traffic on:

- TCP/UDP 53 – DNS
- TCP/UDP 88 – Kerberos authentication
- TCP/UDP 389 – LDAP

11.5.3 Configuring the AWS Client VPN Endpoint with AD Authentication

1. Create a client VPN endpoint. In the AWS Management Console, go to the Amazon VPC console. In Client VPN Endpoints, create a client VPN Endpoint. Specify the following information:
 - Client IPv4 CIDR – It must not overlap with VPC CIDR or the existing VPN CIDR created by Setup.ps1.
 - Server certificate – Select the certificate uploaded by the Setup.ps1 script.
 - Authentication method – Select Active Directory authentication.
 - Choose the AD Connector created earlier.
2. Associate the target network. Associate the VPN endpoint with a VPC public subnet to allow resource access.
3. Add authorization rules. Define which AD groups can access specific networks. Navigate to Authorization Rules and add rules based on group membership.
4. Download VPN Configuration. From the VPN endpoint page, download the Client VPN configuration file. Distribute the file to users for AWS VPN Client setup.
5. Connect and test. Users install the AWS VPN Client, import the configuration file, and connect using their AD credentials.

12 Supported platforms and system requirements

This section lists supported operating systems and system requirements for the following OpenText Server Backup - Public Cloud components:

- *Windows Agent supported platforms, requirements and recommendations below*
- *BMR Media Creator supported platforms, requirements and known issues on page 92*
- *BMR Agent supported platforms, requirements and known issues on page 94*

12.1 Windows Agent supported platforms, requirements and recommendations

This section provides the following information for the Windows Agent:

- *Supported operating systems below*
- *Supported systems and storage on the next page*
- *System requirements on the next page*
- *Product compatibility on the next page*
- *Limitations on page 92*
- *Recommendations on page 92*

The Windows Agent is installed on each Windows server that you want to back up. For more information, see *Downloading and installing the Windows Agent* on page 35.

Supported operating systems

The Windows Agent supports backups and recoveries for servers with the following 64-bit Microsoft Windows Server operating systems, including Server Core installations:

- Windows Server 2025
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016

The Windows Agent can back up servers with Windows operating systems in languages that use ASCII or double-byte characters.

Note: Double-byte characters are not supported for agent passwords used for encryption. Agent passwords can have ASCII characters only, with no spaces or angled brackets < >.

Supported systems and storage

File systems	The Windows Agent can back up servers with the NTFS file system. The Agent is not supported with the ReFS file system.
Roles and services	The Windows Agent can back up servers with the following roles and services: <ul style="list-style-type: none">• Active Directory• Hyper-V
Volumes and storage	<p>The Windows Agent can back up:</p> <ul style="list-style-type: none">• Windows Storage Spaces• Dynamic volumes (recovered as basic disks)• Volumes that are encrypted using BitLocker, if they are unlocked at the time of backup. When unlocked volumes are recovered, they are not encrypted and must be re-encrypted, if desired. <p>The Windows Agent cannot back up:</p> <ul style="list-style-type: none">• iSCSI volumes• Cluster shared volumes• Removable drives

System requirements

Each server where the Windows Agent is installed must meet the following requirements:

- CPU and RAM to meet the basic requirements of your operating system, as prescribed by Microsoft.
- A TCP/IP stack.
- 200 MB of free disk space is required for installing the Windows Agent. Additional space is required for the agent to function. We recommend a total of at least 1 GB of free disk space for the Windows Agent.
- A minimum outbound network bandwidth of 2 Mbps to allow backups to succeed.

Traffic must be allowed to the following URLs on the following ports:

URL	Port	Direction
agentconnector.my.webrootanywhere.com	8087	Outbound
backupdevices.my.webrootanywhere.com	443	Outbound
agentkit.backupconsole.my.webrootanywhere.com	443	Outbound

Product compatibility

The Windows Agent can be installed on the same server as the following OpenText threat protection and detection products:

- Endpoint Protection agent
- DNS Protection agent
- Endpoint Detection and Response agent
- Managed Detection and Response agent

Limitations

- The Windows Agent can back up disks that are as large as 10 TB in size.
- To ensure successful disaster recoveries, back up Windows servers with a maximum of 21 volumes.

Recommendations

- If you use an antivirus program, disable real-time scanning on reads (called "outgoing" in some antivirus products).
- On a virtual machine where the Windows Agent is installed, do not take snapshots of the virtual machine memory. Virtual memory snapshots can interfere with Windows Agent backups, and are generally discouraged in production environments.

12.2 BMR Media Creator supported platforms, requirements and known issues

This section provides the following information for the BMR Media Creator:

- *Supported operating systems* below
- *System requirements* on the next page
- *Required free space* on the next page
- *Known issues* on the next page

The BMR Media Creator is used to create recovery media for recovering Windows servers to hardware or virtual machines. For more information, see *Recovering a Windows server to hardware or to a virtual machine* on page 54.

Supported operating systems

The BMR Media Creator is supported on the following Microsoft Windows 64-bit operating systems:

- Windows Server 2025
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016

System requirements

The following software components must be installed on the system where you run BMR Media Creator:

- Windows Assessment and Deployment Kit (Windows ADK) and the Windows Preinstallation Environment (Windows PE). You must create separate recovery media for restoring systems with Windows Server 2025 or Windows Server 2022, and for restoring systems with Windows Server 2019 or Windows Server 2016. As shown in the following table, the required Windows ADK and Windows PE version depends on the operating system versions that you want to restore.

Operating systems to restore	Required Windows ADK and PE version
Windows Server 2025 or Windows Server 2022	10.1.26100.2454
Windows Server 2019 or Windows Server 2016	10.1.17134

Before creating recovery media, you must uninstall any other Windows ADK and PE version and install the required version. You can download Windows ADK and Windows PE from Microsoft and install them before running the BMR Media Creator, or when you run the BMR Media Creator.

- .NET Framework 4.8 must be installed on the machine where you run the BMR Media Creator. If .NET Framework 4.8 is not present on the machine where you install BMC, you will be prompted to install it.

Required free space

The system where you run BMR Media Creator must have the following free space:

- At least 100 MB of free disk space for BMC installation
- At least 7 GB of free disk space for installing Windows ADK and Windows PE
- At least 500 MB of free disk space for creating an ISO file

The system drive requires free space to uncompress the packages for installation. The environment variables TEMP and TMP use %USERPROFILE% by default. Make sure that %USERPROFILE% points to a drive that has sufficient temporary space.

Known issues

- When you try to create recovery media, the process sometimes fails with an "Error code:1" message. This can occur due to the antivirus program on the computer where you are running the BMR Media Creator.
WORKAROUND: Either run the BMR Media Creator on a computer with a different antivirus program, or uninstall and then reinstall Windows ADK, disable the antivirus program, and run the BMR Media Creator again.

- When creating recovery media using the BMR Media Creator, an *Insufficient memory* error can occur if you try to add a driver with a long path and file name.

12.3 BMR Agent supported platforms, requirements and known issues

This section provides the following information for the BMR (Bare Metal Recovery) Agent:

- *Supported file systems, disks, and partitions* below
- *Limitations* below
- *Known issues* on the next page

The BMR Agent is used to recover entire Windows servers from backups created by the Windows Agent. For more information, see *Recovering a Windows server* on page 66.

Supported file systems, disks, and partitions

Supported file systems	<ul style="list-style-type: none">• NTFS• FAT32 for volumes that are required for the boot process
Supported disk layouts	<ul style="list-style-type: none">• MBR• GPT
Supported OEM partitions	<ul style="list-style-type: none">• 0x12 // EISA partition (Compaq)• 0x84 // Hibernation partition for laptops• 0xA0 // Diagnostic partition on some Hewlett-Packard notebooks• 0xDE // Dell partition• 0xFE // IBM IML partition

Limitations

- The BMR Agent cannot run on 32-bit hardware.
- Volumes that are encrypted using BitLocker, and were unlocked at the time of backup, are not encrypted when they are recovered and must be re-encrypted, if desired.
- BMR Agent is not supported on VMware ESX 4.x.
- UEFI backups cannot be restored to Generation 1 Hyper-V virtual machines, which do not have support for UEFI.
- The BMR Agent can recover a maximum of 21 volumes from a source (backed up) server to a recovery (destination) server. If existing volumes are preserved on the recovery server, the total of:
 - the number of volumes preserved on the recovery server
plus
 - the number of volumes recovered from the source server

can be a maximum of 21 volumes. For example, if you want to preserve 3 volumes on a recovery server, you can recover a maximum of $21-3=18$ volumes from the source server.

Known issues

- When recovering a server with an MBR disk to its original system, if you click the AutoMap button, a message states that the source volume cannot be mapped because there is not enough space available.
WORKAROUND: Drag the MBR disk to the recovery server manually.
- After you recover a computer that has more than one disk, NTFS disks that do not contain the system partition might be offline. This can occur after a recovery with recovery media for Windows Server 2025 or Windows Server 2022.
WORKAROUND: Bring the NTFS disks online using the Disk Management utility or diskpart command interpreter in Windows.
- When recovering a system to a Hyper-V destination machine, the order of the destination machine disks in the BMR wizard is sometimes different than the order of the disks in the virtual machine settings.
- Removable USB drives on the source or recovery (destination) server are counted in the number of disks on the system and could prevent the AutoMap feature from being available—even though removable USB drives are not backed up and cannot be used as recovery destinations.
WORKAROUND: If the AutoMap feature is not available, manually create a recovery plan by dragging volumes from the source to the recovery system. If the removable drive is on the recovery system, remove the drive before the recovery.
- If you try to recover a volume that is formatted with a 2K block size to a disk that has a 4K cluster size, the recovery fails with the following error message: *Cluster must be multiplication of the physical sector size*.
- When you try to recover to a destination disk with an OEM volume, the recovery may fail with the following message: *BMR is not able to get drive letter for mapped volume. Restore cannot proceed further. Please cancel and try again*.
WORKAROUND: Delete all partitions from the destination disk. Change the disk format to GPT and then back to MBR, and then try the restore again.
- When mapping a volume, even if you drag and drop the volume to a larger size destination, you may get the following message: *Volume cannot be mapped. The destination is not of the same size*.
WORKAROUND: Right-click the volume, delete the partition on the destination disk, and try again.
- The BMR Agent may not retrieve the drive letter for a mapped volume if you drag and drop a large number of partitions to a GPT disk. The recovery may not proceed further.
WORKAROUND: Cancel and try again, selecting fewer partitions.