Alibaba Cloud
Elastic Compute Service

FAQ

Issue: 20190424

Legal disclaimer

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

1. **You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.**
2. **No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.**
3. **The content of this document may be changed due to product version upgrades , adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.**
4. **This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults " and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity , applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use**

or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.

5. By law, all the content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of the Alibaba Cloud website, product programs, or content shall be used, modified , reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates . The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates).
6. Please contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 Danger: Resetting will result in the loss of user configuration data.
	This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 Warning: Restarting will cause business interruption. About 10 minutes are required to restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus , page names, and other UI elements.	Click OK.
`Courier font`	It is used for commands.	Run the `cd / d C :/ windows` command to enter the Windows system folder.
Italics	It is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *[-all|-t]*

Style	Description	Example
{} or {a|b}	It indicates that it is a required value, and only one item can be selected.	`swich {stand | slave}`

Contents

1 Common issues

1.1 Block storage

1.2 Images

1.2.1 How do I enable or disable the Meltdown and Spectre patches for Linux images?

This topic describes how Alibaba Cloud ECS responds to the Meltdown and Spectre vulnerabilities. You can learn about our measures for protecting ECS instances against these vulnerabilities.

Context

The Meltdown and Spectre vulnerabilities exist in the Intel chips. Caused by the design flaw of the chip hardware, the vulnerabilities may lead to problems such as leakage of operating system kernel information, unauthorized access to system kernel data by applications, and more. You can go to the CVE website to check the vulnerability IDs:

- *CVE-2017-5753*
- *CVE-2017-5715*
- *CVE-2017-5754*

On January 20, 2018, Alibaba Cloud released a *security vulnerability notice*, describing the vulnerability details and impacts.

This topic describes the Alibaba Cloud public images that have been patched against these vulnerabilities, and how to disable the patches for better instance performance . The default security policy is as follows:

- To protect against the Meltdown vulnerability, Page Table Isolation (PTI) is enabled by default.
- To protect against the Spectre vulnerability, by default No Indirect Branch Restricted Speculation (NOIBRS) is enabled and is integrated with Retpoline and Indirect Branch Prediction Barriers (IBPB).

How to enable or disable the Meltdown patch

The following public images have enabled the Meltdown patch (PTI On):

- CentOS 7.5/7.6
- Debian 9.6/8.10
- Red Hat 7.5/7.6
- SUSE Linux 15
- Ubuntu 18.04
- CoreOS 1911.3.0
- FreeBSD 11.2
- OpenSUSE 15

The above list is subject to change due to updates of Alibaba Cloud public images.

If you find enabling PTI impacts your instance performance, or you have other protective measures, you can disable PTI by following the steps below:

1. Connect to your instance.
2. Do the following according to your Linux distribution:
   - CentOS, Debian, OpenSUSE, Red Hat, SUSE Linux and Ubuntu: Add the kernel parameter `nopti`.
   - CoreOS: Run `vi /usr/share/oem/grub.cfg` to configure `pti=off`.
   - FreeBSD: Run `vi /boot/loader.conf` to configure `vm.pmap.pti=0`.
3. Restart the instance.

How to enable or disable the Spectre patch

Alibaba Cloud currently allows you to configure Indirect Branch Restricted Speculation (IBRS) and IBPB. By default, public images are protected against Spectre through Reptpoline and IBPB. Moreover, IBRS is disabled through the noibrs parameter. The following public images are involved:

- CentOS 7.5/7.6
- Debian 9.6/8.10
- Red Hat 7.5/7.6
- SUSE Linux 15

- Ubuntu 18.04
- CoreOS 1911.3.0
- FreeBSD 11.2
- OpenSUSE 15

The above list is subject to change due to updates of Alibaba Cloud public images.

If you need to restore the default settings of your operating system, or you find the current settings impact your instance performance, or you have other protective measures, you can disable the Spectre patch by following the steps below:

1. Connect to your instance.
2. Perform the corresponding operation according to the instructions in the following table.

Linux distribution	To restore the default settings of Alibaba Cloud images	To restore the default settings of operating systems	To disable the Spectre patch
CentOS	Add the kernel parameter noibrs.	Remove the kernel parameter noibrs.	Add the kernel parameter spectre_v2=off.
Red Hat			
CoreOS	Run `vi /usr/oem/share/grub.cfg` to add the kernel parameter spectre_v2=off.	Remove the kernel parameter spectre_v2=off.	
OpenSUSE	Add the kernel parameter spectre_v2=off.		
Debian	Retpoline and IBPB are enabled by default.	No need to modify the settings.	
Ubuntu			
SUSE Linux	Retpoline is enabled by default.		
FreeBSD	Add the kernel parameter hw.ibrs_disable.	Remove the kernel parameter hw.ibrs_disable.	Add the kernel parameter hw.ibrs_disable.

 Note:

The kernel parameter `noibrs` does not work for OpenSUSE and CoreOS. You need to set `spectre_v2 = off` for them.

3. Restart the instance.

How to detect whether protections are enabled

1. Connect to your instance.
2. From *GitHub spectre-meltdown-checker Repo*, obtain the spectre-meltdown-checker.sh script.
3. Run the following commands in your instance:

```
chmod + x spectre - meltdown - checker . sh
sudo bash spectre - meltdown - checker . sh
```

4. Judge whether the Meltdown or Spectre patch has been enabled according to the script prompts.

Reference

For the following operating systems, you can go to their website for more details:

- *Red Hat*
- *SUSE Linux*
- *Ubuntu*

2 O&M issues in Windows instances

2.1 OS issues

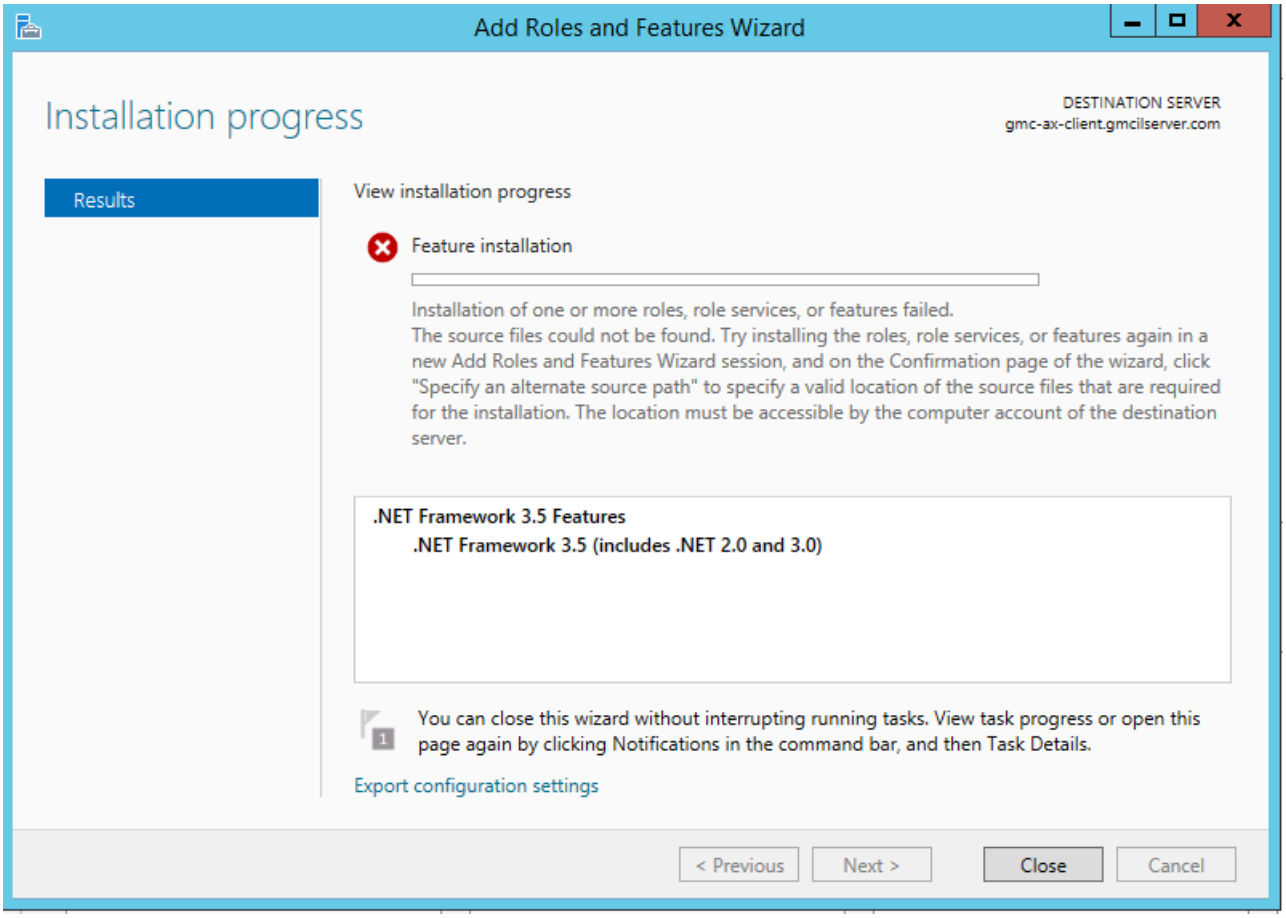
2.1.1 Updates and patches

2.1.1.1 How do I install the .NET Framework 3.5 SP1 in a Windows instance?

When you install the .NET Framework 3.5 SP1 through Server Manager or by other means, if the system prompts you that the source file cannot be found, you can install it through commands by following the instructions below .

Symptom

When .NET Framework 3.5 is being installed in a Windows instance, the following error is displayed:



Cause

To use a Feature on Demand (FOD) in Windows Server 2012 and higher, you need to download the installation package from Windows Update. However, a Windows instance uses Windows Server Update Services (WSUS) to get the updates by default. This results in missing installation and language package files of the .NET Framework, and the system prompts you that Source file cannot be found.

Note:

- The PowerShell commands described in this topic can all be executed through the Cloud Assistant. For more information, see *Cloud Assistant*.
- If you want to automatically install the .NET Framework 3.5 by running PowerShell commands during instance creation, we recommend that you do it with the help of instance user data. For more information, see *User data*.

Windows Server 2008

Open the CMD utility as an administrator and run the following command to enable .NET Framework 3.5 :

```
cmd  / c   start  / w   ocsetup   NET - Framework - Core
```

Windows Server 2008 R2

1. Open the CMD utility as an administrator and run `powershell` to switch to interactive mode.
2. Run the following commands to enable .NET Framework 3.5:

```
Import - Module   Servermana  ger
Add - WindowsFea  ture   Net - Framework - Core
```

Windows Server 2012 R2/2016/1709/1809

1. Open the CMD utility as an administrator and run `powershell` to switch to interactive mode.
2. Run the following commands to modify the registry to set the update source to Windows Update:

```
$ ServicingP  olicy  = " HKLM :\ SOFTWARE \ Microsoft \ Windows \
 CurrentVer  sion \ policies \ Servicing "
 New - Item  $ ServicingP  olicy  - Force
 New - ItemProper  ty  - Path  $ ServicingP  olicy  - Name
 RepairCont  entServerS  ource  - PropertyTy  pe  DWord  - Value
 2  - Force
```

```
New - ItemProper  ty  - Path  $ ServicingP  olicy  - Name
LocalSourc  ePath  - PropertyTy  pe  ExpandStri  ng  - Force
```

3. Run the following commands to enable .NET Framework 3.5:

```
Import - Module  Servermana  ger
Add - WindowsFea  ture  Net - Framework - Core
```

Windows Server 2019

1. Open the CMD utility as an administrator and run `powershell` to switch to interactive mode.
2. Run the following command to enable .NET Framework 3.5:

```
Add - WindowsCap  ability  - Online  - Name  Net - Framework -
Core
```