

<https://customerconnect.vmware.com/home>

Products and Accounts

Knowledge

MAIN CONTENT

Search for topics, products or issues..



Implementing Hypervisor-Specific Mitigations for Microarchitectural Data Sampling (MDS) Vulnerabilities (CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, and CVE-2019-11091) in vSphere (67577)

Take Our Survey

Last Updated: 2/10/2020 Categories: Security Total Views: 57424

Language: English



SUBSCRIBE



81 people found this helpful

Please provide article feedback:

▼ Purpose

This article documents the [Hypervisor-Specific Mitigations](#) enablement process required to address Microarchitectural Data Sampling (MDS) Vulnerabilities identified by CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, and CVE-2019-11091 in vSphere.

Support Assistant

In addition to the [Hypervisor-Specific Mitigations](#) described in this article, [Hypervisor-Assisted Guest Mitigations](#) and [Operating System-Specific Mitigations](#) are also required.

These additional mitigations are documented VMSA-2019-0008.

(<https://customerconnect.vmware.com/home>) Products and Accounts Knowledge

The **Update History** section of this article will be revised if there is a significant change.

Click **Subscribe to Article** in the Actions box to be alerted when new information is added to this document and sign up at our Security-Announce mailing list

(<http://lists.vmware.com/cgi-bin/mailman/listinfo/security-announce>) to receive new and updated VMware Security Advisories.

Introduction to MDS

Intel has disclosed details on a new wave of speculative-execution vulnerabilities known collectively as "Microarchitectural Data Sampling (MDS)" that can occur on Intel microarchitecture prior to 2nd Generation Intel® Xeon® Scalable Processors (formerly known as Cascade Lake). These issues may allow a malicious user who can locally execute code on a system to infer the values of data otherwise protected by architectural mechanisms.

Attack Vector Summary

- Sequential-context attack vector (Inter-VM): a malicious VM can potentially infer recently accessed data of a previous context (hypervisor thread or other VM thread) on either logical processor of a processor core.
- Concurrent-context attack vector (Inter-VM): a malicious VM can potentially infer recently accessed data of a concurrently executing context (hypervisor thread or other VM thread) on the other logical processor of the Hyper-Threading-enabled processor core.

Take Our Survey

Mitigation Summary

- The Sequential-context attack vector (Inter-VM): is mitigated by a Hypervisor update to the product versions listed in VMSA-2019-0008 section 3a. These mitigations are dependent on Intel microcode updates (provided in separate ESXi patches for most Intel hardware platforms) also listed in the advisory. This mitigation is enabled by default and does not impose a significant performance impact.

Support Assistant

- The Concurrent-context attack vector (Inter-VM): is mitigated through enablement of the ESXi Side-Channel-Aware Scheduler Version 1 or Version 2. These options may

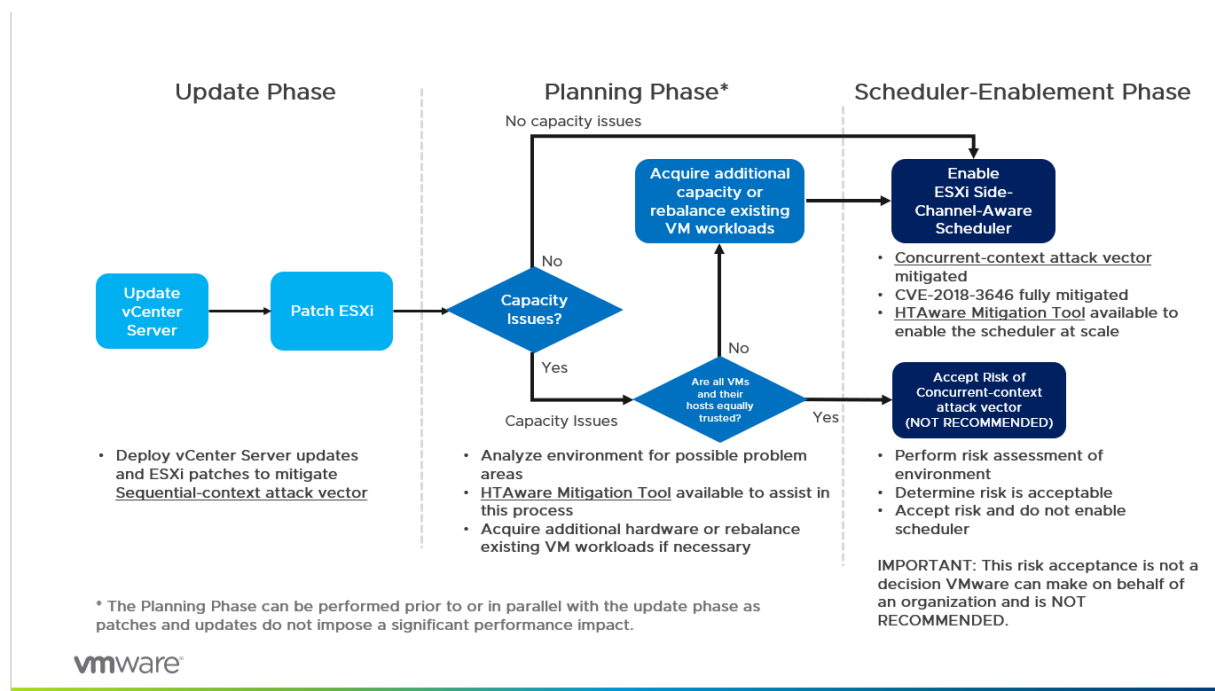
impose a non-trivial performance impact and are not enabled by default.
(<https://customerconnect.vmware.com/home>)

Products and Accounts Knowledge

Important: Disabling Intel Hyperthreading in firmware/BIOS (or by using VMkernel.Boot.Hyperthreading) after applying vSphere updates and patches is not recommended.

✓ Resolution

The Inter-VM mitigation process for MDS is divided into three phases:



Take Our Survey

1. Update Phase: Apply vSphere Updates and Patches

The Inter-VM Sequential-context attack vector is mitigated by a vSphere update to the product versions listed in VMware Security Advisory VMSA-2019-0008. This mitigation is dependent on Intel microcode updates (provided in separate ESXi patches for most Intel hardware platforms) which are also documented in VMSA-2019-0008. This mitigation is enabled by default and does not impose a significant performance impact.

Note: As displayed in the workflow above, vCenter Server should be updated prior to applying ESXi patches. Notification messages were previously issued in the patches to explain that the ESXi Side-Channel-Aware Scheduler must be enabled to mitigate Inter-VM Concurrent-context attack vectors. If ESXi is updated prior to vCenter you may receive cryptic notification messages relating to this. After vCenter has been

updated, the notifications will be shown correctly.

(<https://customerconnect.vmware.com/home>)

Products and Accounts

Knowledge

2. Planning Phase: Assess Your Environment

Inter-VM Concurrent-context attack vectors are mitigated through enablement of the ESXi Side-Channel-Aware Scheduler which is included in the updates and patches listed in VMSA-2019-0008. This scheduler is not enabled by default. Enablement of this scheduler may impose a non-trivial performance impact on applications running in a vSphere environment. The goal of the Planning Phase is to understand if your current environment has sufficient CPU capacity to enable the scheduler without operational impact.

The following list summarizes potential problem areas after enabling the ESXi Side-Channel-Aware Scheduler:

- VMs configured with vCPUs greater than the physical cores available on the ESXi host
- VMs configured with custom affinity or NUMA settings
- VMs with latency-sensitive configuration
- ESXi hosts with Average CPU Usage greater than 70%
- Hosts with custom CPU resource management options enabled
- HA Clusters where a rolling upgrade will increase Average CPU Usage above 100%

Take Our Survey

Important: The above list is meant to be a brief overview of potential problem areas related to enablement of the ESXi Side-Channel-Aware Scheduler. The VMware Performance Team has provided an in-depth guide as well as performance data in KB55767 (</s/article/55767>). It is strongly suggested to thoroughly review this document prior to enablement of the scheduler.

Note: It may be necessary to acquire additional hardware, or rebalance existing workloads, before enablement of the ESXi Side-Channel-Aware Scheduler. Organizations can choose not to enable the ESXi Side-Channel-Aware Scheduler after by accepting the risk posed by the Concurrent-context attack vector. This is NOT RECOMMENDED and VMware cannot make this decision on behalf of an organization.

Support Assistant

3. Scheduler-Enablement Phase:

(<https://customerconnect.vmware.com/home>)

Products and Accounts

Knowledge

1. Enable the ESXi Side-Channel-Aware Scheduler in ESXi 5.5, 6.0, 6.5, and 6.7 prior to 6.7u2.

After addressing the potential problem areas described above during the Planning Phase, the ESXi Side-Channel-Aware Scheduler must be enabled to mitigate Inter-VM Concurrent-context attack vectors. The scheduler can be enabled on an individual ESXi host via the advanced configuration option `hyperthreadingMitigation`.

Note: Enabling this option will result in the vSphere UI reporting only a single logical processor per physical core; halving the number of logical processors if Hyperthreading was previously enabled. In addition Hyperthreading may be reported as 'Disabled' in various configuration tabs.

Enabling the ESXi Side-Channel-Aware Scheduler using the vSphere Web Client or vSphere Client

1. Connect to the vCenter Server using either the vSphere Web or vSphere Client.
2. Select an ESXi host in the inventory.
3. Click the **Manage** (5.5/6.0) or **Configure** (6.5/6.7) tab.
4. Click the **Settings** sub-tab (5.5/6.0) or find the **System** section in the middle panel (6.5/6.7).
5. Under the System heading, click **Advanced System Settings**.
6. Click in the Filter box and search for `VMkernel.Boot.hyperthreadingMitigation`
7. Select the setting by name and click the **Edit** pencil icon.
8. Change the configuration option to true (default: false).
9. Click **OK**.
10. Reboot the ESXi host for the configuration change to go into effect.

Enabling the ESXi Side-Channel-Aware Scheduler using ESXi Embedded Host Support Assistant Client

1. Connect to the ESXi host by opening a web browser to

Take Our Survey

https://HOSTNAME.
(https://customerconnect.vmware.com/home) Products and Accounts Knowledge

2. Click the **Manage** tab.
3. Click the **Advanced settings** sub-tab
4. Click in the Filter box and search
for `VMkernel.Boot.hyperthreadingMitigation`
5. Select the setting by name and click the **Edit** pencil icon
6. Change the configuration option to true (default: false)
7. Click **Save**.
8. Reboot the ESXi host for the configuration change to go into effect.

Enable ESXi Side-Channel-Aware Scheduler setting using ESXCLI

1. SSH to an ESXi host or open a console where the remote ESXCLI is installed. For more information, see the <http://www.vmware.com/support/developer/vcli/> (<http://www.vmware.com/support/developer/vcli/>)
2. Check the current runtime value of the HTAware Mitigation Setting by running `esxcli system settings kernel list -o hyperthreadingMitigation`
3. To enable HT Aware Mitigation, run this command:

```
esxcli system settings kernel set -s
hyperthreadingMitigation -v TRUE
```

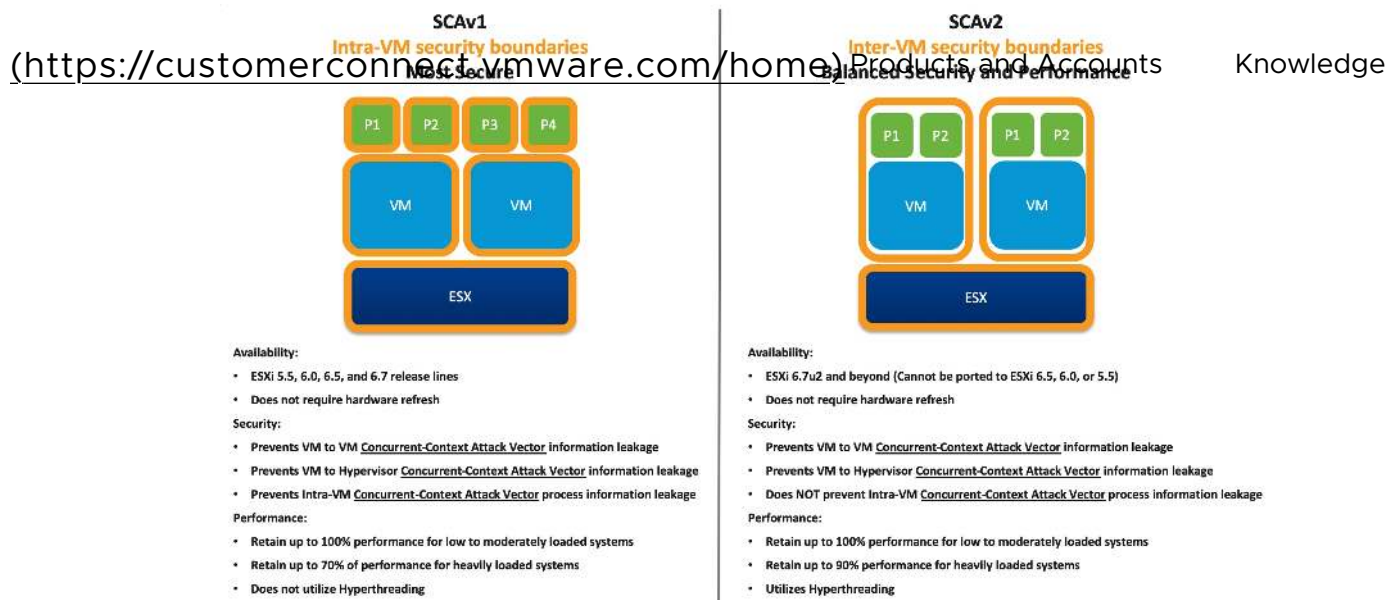
4. Reboot the ESXi host for the configuration change to go into effect.

2. Enable the ESXi Side-Channel-Aware Scheduler (SCAv1) or the ESXi Side-Channel-Aware Scheduler v2 (SCAv2) in ESXi 6.7u2 (13006603) or later

Note: ESXi 6.7u2 (13006603) and future release lines of ESXi include the [ESXi Side-Channel-Aware Scheduler v2](#). Prior release lines such as 6.5, 6.0, and 5.5 cannot accommodate this new scheduler.

Take Our Survey

Support Assistant



VMware has published a white paper entitled Performance of vSphere 6.7 Scheduling Options (<https://www.vmware.com/techpapers/2018/scheduler-options-vsphere67u2-perf.html>) which provides a more detailed look into the performance differences between SCAv1 and SCAv2. Please review this document before continuing.

Enabling the ESXi Side-Channel-Aware Scheduler (SCAv1) using the vSphere Web Client or vSphere Client

1. Connect to the vCenter Server using either the vSphere Web or vSphere Client.
2. Select an ESXi host in the inventory.
3. Click the **Configure** tab.
4. Under the System heading, click **Advanced System Settings**.
5. Click **Edit**.
6. Click in the Filter box and search for `VMkernel.Boot.hyperthreadingMitigation`
7. Select the setting by name
8. Change the configuration option to true (default: false).
9. Click in the Filter box and search for `VMkernel.Boot.hyperthreadingMitigationIntraVM`
10. Change the configuration option to true (default: false)
11. Click **OK**.
12. Reboot the ESXi host for the configuration change to go into effect.

Take Our Survey

Support Assistant

Enabling the ESXi Side-Channel-Aware Scheduler (SCAv1) using ESXi (<https://customerconnect.vmware.com/home>)

Embedded Host Client

Products and Accounts

Knowledge

1. Connect to the ESXi host by opening a web browser to `https://HOSTNAME`.
2. Click **Manage** under host navigator
3. Click the **Advanced settings** Tab
4. Use the search box to find `VMkernel.Boot.hyperthreadingMitigation`
5. Select the `VMkernel.Boot.hyperthreadingMitigation` setting and click the **Edit** Option
6. Change the configuration option to true (default: false)
7. Click **Save**.
8. Use the search box to find `VMkernel.Boot.hyperthreadingMitigationIntraVM`
9. Select the `VMkernel.Boot.hyperthreadingMitigationIntraVM` setting and click the **Edit** Option
10. Change the configuration option to true (default: true).
11. Click **Save**.
12. Reboot the ESXi host for the configuration change to go into effect.

Enable ESXi Side-Channel-Aware Scheduler (SCAv1) using ESXCLI

1. SSH to an ESXi host or open a console where the remote ESXCLI is installed. For more information, see the <http://www.vmware.com/support/developer/vcli/> (<http://www.vmware.com/support/developer/vcli/>).
2. Check the current runtime values by running `esxcli system settings kernel list -o hyperthreadingMitigation` and `esxcli system settings kernel list -o hyperthreadingMitigationIntraVM`
3. To enable the ESXi Side-Channel-Aware Scheduler Version 1, run these commands:

```
esxcli system settings kernel set -s  
hyperthreadingMitigation -v TRUE
```

Support Assistant

Take Our Survey

`esxcli system settings kernel set -s hypervthreadingMitigationIntraVM -v TRUE`
(<https://customerconnect.vmware.com/home>) Products and Accounts Knowledge

4. Reboot the ESXi host for the configuration change to go into effect.

Enabling the ESXi Side-Channel-Aware Scheduler Version 2 (SCAv2) using the vSphere Web Client or vSphere Client

1. Connect to the vCenter Server using either the vSphere Web or vSphere Client.
2. Select an ESXi host in the inventory.
3. Click the **Configure** tab.
4. Under the System heading, click **Advanced System Settings**.
5. Click **Edit**.
6. Click in the Filter box and search for `VMkernel.Boot.hypervthreadingMitigation`
7. Select the setting by name
8. Change the configuration option to true (default: false).
9. Click in the Filter box and search for `VMkernel.Boot.hypervthreadingMitigationIntraVM`
10. Change the configuration option to false (default: true).
11. Click **OK**.
12. Reboot the ESXi host for the configuration change to go into effect.

Enabling the ESXi Side-Channel-Aware Scheduler Version 2 (SCAv2) using ESXi Embedded Host Client

1. Connect to the ESXi host by opening a web browser to `https://HOSTNAME`.
2. Click **Manage** under host navigator
3. Click the **Advanced Settings** tab
4. Use the search box to find `VMkernel.Boot.hypervthreadingMitigation`
5. Select the `VMkernel.Boot.hypervthreadingMitigation` setting and click the **Edit** option
6. Change the configuration option to true (default: false)
7. Click **Save**.
8. Use the search box to find `VMkernel.Boot.hypervthreadingMitigationIntraVM`

Support Assistant

Take Our Survey

9. Select <https://customerconnect.vmware.com/home> Products and Accounts Knowledge and click the **Edit** option.
10. Change the configuration option to false (default: true).
11. Click **Save**.
12. Reboot the ESXi host for the configuration change to go into effect.

Enable ESXi Side-Channel-Aware Scheduler Version 2 (SCAv2) using ESXCLI

1. SSH to an ESXi host or open a console where the remote ESXCLI is installed. For more information, see the <http://www.vmware.com/support/developer/vcli/> (<http://www.vmware.com/support/developer/vcli/>)
2. Check the current runtime values by running `esxcli system settings kernel list -o hyperthreadingMitigation` and `esxcli system settings kernel list -o hyperthreadingMitigationIntraVM`
3. To enable the ESXi Side-Channel-Aware Scheduler Version 2 run these commands:

```
esxcli system settings kernel set -s
hyperthreadingMitigation -v TRUE
```

```
esxcli system settings kernel set -s
hyperthreadingMitigationIntraVM -v FALSE
```

4. Reboot the ESXi host for the configuration change to go into effect.

ESXi 6.7u2 (and later) Scheduler Configuration Summary

hyperthreadingMitigation	hyperthreadingMitigationIntraVM	Scheduler Enabled
FALSE	TRUE or FALSE	Default scheduler (unmitigated)
TRUE	TRUE	SCAv1

Take Our Survey

TRUE (https://customerconnect.vmware.com/home)	FALSE	SCAv2	Products and Accounts	Knowledge
---	-------	-------	-----------------------	-----------

HTAware Mitigation Tool

VMware has provided a tool to assist in performing both the **Planning Phase** and the **Scheduler-Enablement** Phase at scale. This tool has been updated to include SCAv2 support and can be found in KB56931 (/s/article/56931) along with detailed instructions on its usage, capabilities, and limitations.

Table 1: Affected Intel Processors Supported by ESXi




Intel Code Name	FMS	Intel Brand Names
Nehalem-EP	0x106a5	Intel Xeon 35xx Series; Intel Xeon 55xx Series
Lynnfield	0x106e5	Intel Xeon 34xx Lynnfield Series
Clarkdale	0x20652	Intel i3/i5 Clarkdale Series; Intel Xeon 34xx Clarkdale Series
Arrandale	0x20655	Intel Core i7-620LE Processor
Sandy Bridge DT	0x206a7	Intel Xeon E3-1100 Series; Intel Xeon E3-1200 Series; Intel i7-2655-LE Series; Intel i3-2100 Series
Westmere EP	0x206c2	Intel Xeon 56xx Series; Intel Xeon 36xx Series
Sandy Bridge EP	0x206d7	Intel Pentium 1400 Series; Intel Xeon E5-1400 Series; Intel Xeon E5-1600 Series; Intel Xeon E5-2400 Series; Intel Xeon E5-2600 Series; Intel Xeon E5-4600 Series
Nehalem EX	0x206e6	Intel Xeon 65xx Series; Intel Xeon 75xx Series

Take Our Survey

Support Assistant

(https://customerconnect.vmware.com/home)		Intel Xeon E7-8800 Series; Intel Xeon E7-2800 Series	Products and Accounts Knowledge
Ivy Bridge DT	0x306a9	Intel i3-3200 Series; Intel i7-3500-LE/UE, Intel i7-3600-QE, Intel Xeon E3-1200-v2 Series; Intel Xeon E3-1100-C-v2 Series; Intel Pentium B925C	
Haswell DT	0x306c3	Intel Xeon E3-1200-v3 Series	
Ivy Bridge EP	0x306e4	Intel Xeon E5-4600-v2 Series; Intel Xeon E5-2400-v2 Series; Intel Xeon E5-2600-v2 Series; Intel Xeon E5-1400-v2 Series; Intel Xeon E5-2600-v2 Series	
Ivy Bridge EX	0x306e7	Intel Xeon E7-8800/4800/2800-v2 Series	
Haswell EP	0x306f2	Intel Xeon E5-2400-v3 Series; Intel Xeon E5-1400-v3 Series; Intel Xeon E5-1600-v3 Series; Intel Xeon E5-2600-v3 Series; Intel Xeon E5-4600-v3 Series	
Haswell EX	0x306f4	Intel Xeon E7-8800/4800-v3 Series	
Broadwell H	0x40671	Intel Core i7-5700EQ; Intel Xeon E3-1200-v4 Series	
Avoton	0x406d8	Intel Atom C2300 Series; Intel Atom C2500 Series; Intel Atom C2700 Series	
Broadwell EP/EX	0x406f1	Intel Xeon E7-8800/4800-v4 Series; Intel Xeon E5-4600-v4 Series; Intel Xeon E5-2600-v4 Series; Intel Xeon E5-1600-v4 Series	
Skylake SP	0x50654	Intel Xeon Platinum 8100 (Skylake-S) Series; Intel Xeon Gold 6100/5100 (Skylake-SP) Series Intel Xeon Silver 4100, Bronze 3100 (Skylake-SP) Series	Support Assistant

Take Our Survey

https://customerconnect.vmware.com/home		Products and Accounts	Knowledge
Broadwell DE	Ox50662	Intel Xeon D-1500 Series	
Broadwell DE	Ox50663	Intel Xeon D-1500 Series	
Actions			
Broadwell DE	Ox50664	Intel Xeon D-1500 Series	
 Copy link to clipboard			
Broadwell NS	Ox50665	Intel Xeon D-1500 Series	
 Print			
 Language: English		English	
Skylake H/S	Ox506e3	Intel Xeon E3-1500-v5 Series; Intel Xeon E3-1200-v5 Series	
Kaby Lake H/S/X	Ox906e9	Intel Xeon E3-1200-v6	
Additional Resources			

Ask The Community

Get answers quickly from VMware experts in the community

Post Subject

Type your question here

CONTINUE IN COMMUNITIES

Take Our Survey

Related Products:

VMware vSphere ESXi
Datacenter

Related Versions:

VMware vSphere ESXi 7.0.0
VMware vSphere ESXi 6.7
VMware vSphere ESXi 6.5

Support Assistant

VMware vSphere ESXi 6.0

VMware vSphere ESXi 5.5

<https://customerconnect.vmware.com/home>

Products and Accounts

Knowledge

<https://twitter.com/VMware><https://www.facebook.com/vmware/><https://www.linkedin.com/company/vmware/><https://www.youtube.com/user/vmwaretv>

Copyright © 2023 VMware, Inc. All rights reserved.

Terms of Use (<https://customerconnect.vmware.com/web/vmware/terms-of-use?mode=view>)

Your California Privacy Rights (<https://www.vmware.com/help/privacy/california-privacy-rights.html>)

Privacy (<https://www.vmware.com/help/privacy.html>)

Accessibility (<https://www.vmware.com/accessibility.html>)

Your Opt-Out Rights

[Take Our Survey](#)

Support Assistant