Reference

AWS Windows AMIs

AWS Windows AMIs: Reference

Table of Contents

AWS Windows AMI reference

AWS provides a set of publicly available Amazon Machine Images (AMIs) that contain software configurations specific to the Windows platform.

You can quickly start building and deploying your applications with Amazon EC2 by using these AMIs. First choose the AMI that meets your specific requirements, and then launch an instance using that AMI. You retrieve the password for the administrator account and then log in to the instance using Remote Desktop Connection, just as you would with any other Windows Server.

In general, the AWS Windows AMIs are configured with the default settings used by the Microsoft installation media. However, Amazon does apply some customizations. For example, the AWS Windows AMIs come with the following software and drivers:

- EC2Launch v2 (Windows Server 2022 and 2025)
- EC2Launch v1 (Windows Server 2016 and 2019)
- EC2Config (through Windows Server 2012 R2)
- AWS Systems Manager
- AWS CloudFormation
- AWS Tools for Windows PowerShell
- Network drivers (SRIOV, ENA, Citrix PV)
- Storage drivers (NVMe, AWS PV, Citrix PV)
- Graphics drivers (NVidia GPU, Elastic GPU)

With the Windows fast launch feature, you can configure pre-provisioned snapshots to launch instances up to 65% faster. For more information, see Configure Windows fast launch for your Windows Server AMI in the *Amazon EC2 User Guide*.

To view changes to each release of the AWS Windows AMIs, including SQL Server updates, see the AWS Windows AMI version history.

Specialized AWS Windows AMIs

In addition to its standard operating system version AMIs, Amazon creates the following types of specialized AWS Windows AMIs:

SQL Server license-included AMIs

Launching an instance from a Windows AMI with Microsoft SQL Server enables you to run the instance as a database server. For more information, see AWS Windows Server license-included SQL Server AMIs.

STIG Hardened AMIs

STIG Hardened EC2 Windows Server AMIs are pre-configured with over 160 required security settings to help ensure that the instances that you launch follow the latest guidelines for STIG compliance. For more information, see STIG Hardened AWS Windows Server AMIs.

NitroTPM enabled AMIs

Amazon creates a set of AMIs that are pre-configured with NitroTPM and UEFI Secure Boot requirements. For more information, see AWS Windows Server NitroTPM enabled AMIs.

You can also create your own customized AMI from one of the AWS Windows AMIs with EC2 Image Builder. For more information, see the EC2 Image Builder User Guide.

We recommend PowerShell for the command line examples in this section. To install PowerShell in your environment, see the Installation page in the *AWS Tools for PowerShell (version 4) User Guide*.

> **Note**
>
> Not all AMIs are available in all Regions.

Find an AWS Windows AMI

Each of the specialized AMI pages linked above has its own filtered search examples, as follows:

- Find Windows Server AMIs with Microsoft SQL Server
- Find a STIG Hardened AMI
- Find Windows Server AMIs configured with NitroTPM and UEFI Secure Boot

You can also search for the latest Windows AMIs that include the EC2Launch v2 agent, as shown in the following PowerShell example:

```
Get-SSMLatestEC2Image `
```

```
    -Path ami-windows-latest `
    -ImageName EC2LaunchV2-Windows* | `
Sort-Object Name
```

Note

If this command doesn't run in your environment, you might be missing a PowerShell module. For more information about this command, see Get-SSMLatestEC2Image Cmdlet. Alternatively, you can use the CloudShell console and run `pwsh` to bring up a PowerShell prompt that already has all of the AWS tools installed. For more information, see the AWS CloudShell User Guide.

Find an AWS Windows AMI in a specific language

The following language-specific AWS Windows AMIs are included in the monthly release:

- English
- Japanese
- Chinese
- Korean
- Czech
- Dutch
- French
- German
- Hungarian
- Italian
- Polish
- Russian
- Portuguese
- Spanish
- Swedish
- Turkish

The following example uses PowerShell to search for the latest English language AWS Windows AMIs:

```
Get-SSMLatestEC2Image `
    -Path ami-windows-latest `
    -ImageName *Windows_Server-*English* | `
Sort-Object Name
```

Note

If this command doesn't run in your environment, you might be missing a PowerShell module. For more information about this command, see Get-SSMLatestEC2Image Cmdlet. Alternatively, you can use the CloudShell console and run pwsh to bring up a PowerShell prompt that already has all of the AWS tools installed. For more information, see the AWS CloudShell User Guide.

AWS Windows Server license-included SQL Server AMIs

AWS Windows AMIs with Microsoft SQL Server include one of the following SQL Server editions. Launching an instance from a Windows AMI with Microsoft SQL Server enables you to run the instance as a database server.

- SQL Enterprise Edition
- SQL Server Standard
- SQL Server Express
- SQL Server Web

For more information about running Microsoft SQL Server on EC2, see the Microsoft SQL Server on Amazon EC2 User Guide.

Each AWS Windows AMIs with Microsoft SQL Server AMI also includes the following features:

- Automatic Windows and SQL Server updates
- SQL Server Management Studio included
- Preconfigured SQL Server service accounts

Find Windows Server AMIs with Microsoft SQL Server

AWS managed AMIs always include the AMI creation date as part of the name. The best way to ensure that your search returns the AMIs that you're looking for is to add date filtering for the name. Use one of the following command line options to find an AMI.

AWS CLI

Find the latest SQL AMIs

The following example retrieves a list of the latest Windows Server AMIs that include Microsoft SQL Server.

```
aws ssm get-parameters-by-path \
    --path "/aws/service/ami-windows-latest" \
    --recursive \
    --query 'Parameters[*].{Name:Name,Value:Value}' \
    --output text | grep ".*Windows_Server-.*SQL.*" | sort
```

Find a specific AMI

The following example retrieves Windows Server AMIs with Microsoft SQL Server by filtering on the AMI name, the owner, the platform, and the creation date (year and month). Output is formatted as a table with columns for the AMI name and image ID.

```
aws ec2 describe-images \
    --owners amazon \
    --filters \
        "Name=name,Values=*SQL*" \
        "Name=platform,Values=windows" \
        "Name=creation-date,Values=2025-05*" \
    --query 'Images[].[Name,ImageId]' \
    --output text | sort
```

PowerShell (recommended)

Find the latest SQL AMIs

The following example retrieves a list of the latest Windows Server AMIs that include Microsoft SQL Server.

```
Get-SSMLatestEC2Image `
```

```
    -Path ami-windows-latest `
    -ImageName *Windows_Server-*SQL* | `
Sort-Object Name
```

> **Note**
>
> If this command doesn't run in your environment, you might be missing a PowerShell module. For more information about this command, see Get-SSMLatestEC2Image Cmdlet.
> Alternatively, you can use the CloudShell console and run pwsh to bring up a PowerShell prompt that already has all of the AWS tools installed. For more information, see the AWS CloudShell User Guide.

Find a specific AMI

The following example retrieves Windows Server AMIs with Microsoft SQL Server by filtering on the AMI name, the owner, the platform, and the creation date (year and month). Output is formatted as a table with columns for the AMI name and image ID.

```
Get-EC2Image `
    -Owner amazon `
    -Filter @(
        @{Name = "name"; Values = @("*SQL*")},
        @{Name = "owner-alias"; Values = @("amazon")},
        @{Name = "platform"; Values = "windows"},
        @{Name = "creation-date"; Values = @("2025-05*")}
    ) | `
Sort-Object Name |`
Format-Table Name, ImageID -AutoSize
```

STIG Hardened AWS Windows Server AMIs

Security Technical Implementation Guides (STIGs) are the configuration standards created by the Defense Information Systems Agency (DISA) to secure information systems and software. DISA documents three levels of compliance risk, known as categories:

- **Category I** — The highest level of risk. It covers the most severe risks, and includes any vulnerability that can result in a loss of confidentiality, availability, or integrity.

- **Category II** — Medium risk.
- **Category III** — Low risk.

Each compliance level includes all STIG settings from lower levels. This means that the highest level includes all applicable settings from all levels.

To ensure that your systems are compliant with STIG standards, you must install, configure, and test a variety of security settings. STIG Hardened EC2 Windows Server AMIs are pre-configured with over 160 required security settings. Amazon EC2 supports the following operating systems for STIG Hardened AMIs:

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

The STIG Hardened AMIs include updated Department of Defense (DoD) certificates to help you get started and achieve STIG compliance. STIG Hardened AMIs are available in all commercial AWS and GovCloud (US) Regions. You can launch instances from these AMIs directly from the Amazon EC2 console. They are billed using standard Windowspricing. There are no additional charges for using STIG Hardened AMIs.

The following sections list the STIG settings that Amazon applies to WindowsOperating Systems and components.

Topics

Find a STIG Hardened AMI

You can search for a STIG Hardened EC2 Windows Server AMI when you launch an instance from the EC2 console, or you can search for an AMI in the CLI or in PowerShell, as follows.

Name patterns for STIG Hardened Windows AMIs

- Windows_Server-2022-English-STIG-Full-*YYYY.MM.DD*
- Windows_Server-2022-English-STIG-Core-*YYYY.MM.DD*
- Windows_Server-2019-English-STIG-Full-*YYYY.MM.DD*
- Windows_Server-2019-English-STIG-Core-*YYYY.MM.DD*
- Windows_Server-2016-English-STIG-Full-*YYYY.MM.DD*
- Windows_Server-2016-English-STIG-Core-*YYYY.MM.DD*
- Windows_Server-2012-R2-English-STIG-Full-*YYYY.MM.DD*
- Windows_Server-2012-R2-English-STIG-Core-*YYYY.MM.DD*

Console

You can select an AMI from the **Community AMIs** tab when you launch an instance, as follows.

Launch an EC2 instance with a STIG Hardened Windows Server AMI

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. Choose **Instances** from the navigation pane. This opens a list of your EC2 instances in the current AWS Region.
3. Choose **Launch instances** from the upper right corner above the list. This opens the **Launch an instance** page.
4. To find a STIG Hardened AMI, choose **Browse more AMIs** on the right side of the **Application and OS Images (Amazon Machine Image)** section. This displays an advanced AMI search.
5. Select the **Community AMIs** tab, and enter part or all of one of the following name patterns in the search bar. Our AMIs indicate that they are "provided by Amazon."

> **Note**
>
> The date suffix for the AMI (*YYYY.MM.DD*) is the date when the latest version was created. You can search for the version without the date suffix.

AWS CLI

Find the latest STIG AMIs

The following example retrieves a list of the latest STIG Hardened Windows Server AMIs.

```
aws ssm get-parameters-by-path \
    --path "/aws/service/ami-windows-latest" \
    --recursive \
    --query 'Parameters[*].{Name:Name,Value:Value}' \
    --output text | grep "Windows_Server-.*STIG" | sort
```

Find a specific AMI

The following example retrieves STIG Hardened Windows Server AMIs by filtering on the AMI name, the owner, the platform, and the creation date (year and month). Output is formatted as a table with columns for the AMI name and image ID.

```
aws ec2 describe-images \
    --owners amazon \
    --filters \
        "Name=name,Values=*STIG*" \
        "Name=platform,Values=windows" \
        "Name=creation-date,Values=2025-05*" \
    --query 'Images[].[Name,ImageId]' \
    --output text | sort
```

PowerShell

Find the latest STIG AMIs

The following example retrieves a list of the latest STIG Hardened Windows Server AMIs.

```
Get-SSMLatestEC2Image `
```

```
    -Path ami-windows-latest `
    -ImageName *Windows_Server-*STIG* | `
Sort-Object Name
```

> **Note**
>
> If this command doesn't run in your environment, you might be missing a PowerShell module. For more information about this command, see Get-SSMLatestEC2Image Cmdlet.
> Alternatively, you can use the CloudShell console and run pwsh to bring up a PowerShell prompt that already has all of the AWS tools installed. For more information, see the AWS CloudShell User Guide.

Find a specific AMI

The following example retrieves STIG Hardened Windows Server AMIs by filtering on the AMI name, the owner, the platform, and the creation date (year and month). Output is formatted as a table with columns for the AMI name and image ID.

```
Get-EC2Image `
    -Owner amazon `
    -Filter @(
        @{Name = "name"; Values = @("*STIG*")},
        @{Name = "owner-alias"; Values = @("amazon")},
        @{Name = "platform"; Values = "windows"},
        @{Name = "creation-date"; Values = @("2025-05*")}
    ) | `
Sort-Object Name |`
Format-Table Name, ImageID -AutoSize
```

Core and base operating systems

STIG Hardened EC2 AMIs are designed for use as standalone servers, and have the highest level of STIG settings applied.

The following list contains STIG settings that apply for STIG Hardened Windows AMIs. Not all settings apply in all cases. For example, some STIG settings might not apply to standalone servers.

Organization-specific policies can also affect which settings apply, such as a requirement for administrators to review document settings.

For a complete list of Windows STIGs, see the STIGs Document Library. For information about how to view the complete list, see STIG Viewing Tools.

Windows Server 2022 STIG Version 2 Release 4

This release includes the following STIG settings for Windows operating systems:

V-254335, V-254336, V-254337, V-254338, V-254351, V-254357, V-254363, V-254481, V-254247, V-254265, V-254269, V-254270, V-254271, V-254272, V-254273, V-254274, V-254276, V-254277, V-254278, V-254285, V-254286, V-254287, V-254288, V-254289, V-254290, V-254291, V-254292, V-254300, V-254301, V-254302, V-254303, V-254304, V-254305, V-254306, V-254307, V-254308, V-254309, V-254310, V-254311, V-254312, V-254313, V-254314, V-254315, V-254316, V-254317, V-254318, V-254319, V-254320, V-254321, V-254322, V-254323, V-254324, V-254325, V-254326, V-254327, V-254328, V-254329, V-254330, V-254331, V-254332, V-254333, V-254334, V-254339, V-254341, V-254342, V-254344, V-254345, V-254346, V-254347, V-254348, V-254349, V-254350, V-254355, V-254356, V-254356, V-254358, V-254359, V-254360, V-254361, V-254362, V-254364, V-254365, V-254366, V-254367, V-254368, V-254369, V-254370, V-254371, V-254372, V-254373, V-254375, V-254376, V-254377, V-254379, V-254380, V-254382, V-254383, V-254384, V-254431, V-254432, V-254433, V-254434, V-254435, V-254436, V-254438, V-254439, V-254442, V-254443, V-254444, V-254445, V-254449, V-254450, V-254451, V-254452, V-254453, V-254454, V-254455, V-254456, V-254459, V-254460, V-254461, V-254462, V-254463, V-254464, V-254468, V-254470, V-254471, V-254472, V-254473, V-254476, V-254477, V-254478, V-254479, V-254480, V-254482, V-254483, V-254484, V-254485, V-254486, V-254487, V-254488, V-254489, V-254490, V-254493, V-254494, V-254495, V-254497, V-254499, V-254501, V-254502, V-254503, V-254504, V-254505, V-254507, V-254508, V-254509, V-254510, V-254511, V-254512, V-254293, V-254352, V-254353, V-254354, V-254374, V-254378, V-254381, V-254446, V-254465, V-254466, V-254467, V-254469, V-254474, V-254475, and V-254500

Windows Server 2019 STIG Version 3 Release 4

This release includes the following STIG settings for Windows operating systems:

V-205691, V-205819, V-205858, V-205859, V-205860, V-205870, V-205871, V-205923, V-205625, V-205626, V-205627, V-205629, V-205630, V-205633, V-205634, V-205635, V-205636, V-205637, V-205638, V-205639, V-205643, V-205644, V-205648, V-205649,

V-205650, V-205651, V-205652, V-205655, V-205656, V-205659, V-205660, V-205662, V-205671, V-205672, V-205673, V-205675, V-205676, V-205678, V-205679, V-205680, V-205681, V-205682, V-205683, V-205684, V-205685, V-205686, V-205687, V-205688, V-205689, V-205690, V-205692, V-205693, V-205694, V-205697, V-205698, V-205708, V-205709, V-205712, V-205714, V-205716, V-205717, V-205718, V-205719, V-205720, V-205722, V-205729, V-205730, V-205733, V-205747, V-205751, V-205752, V-205754, V-205756, V-205758, V-205759, V-205760, V-205761, V-205762, V-205764, V-205765, V-205766, V-205767, V-205768, V-205769, V-205770, V-205771, V-205772, V-205773, V-205774, V-205775, V-205776, V-205777, V-205778, V-205779, V-205780, V-205781, V-205782, V-205783, V-205784, V-205795, V-205796, V-205797, V-205798, V-205801, V-205808, V-205809, V-205810, V-205811, V-205812, V-205813, V-205814, V-205815, V-205816, V-205817, V-205821, V-205822, V-205823, V-205824, V-205825, V-205826, V-205827, V-205828, V-205830, V-205832, V-205833, V-205834, V-205835, V-205836, V-205837, V-205838, V-205839, V-205840, V-205841, V-205842, V-205861, V-205863, V-205865, V-205866, V-205867, V-205868, V-205869, V-205872, V-205873, V-205874, V-205911, V-205912, V-205915, V-205916, V-205917, V-205918, V-205920, V-205921, V-205922, V-205924, V-205925, V-236001, V-257503, V-205653, V-205654, V-205711, V-205713, V-205724, V-205725, V-205757, V-205802, V-205804, V-205805, V-205806, V-205849, V-205908, V-205913, V-205914, and V-205919

Windows Server 2016 STIG Version 2 Release 10

This release includes the following STIG settings for Windows operating systems:

V-224916, V-224917, V-224918, V-224919, V-224931, V-224942, V-225060, V-224850, V-224852, V-224853, V-224854, V-224855, V-224856, V-224857, V-224858, V-224859, V-224866, V-224867, V-224868, V-224869, V-224870, V-224871, V-224872, V-224873, V-224881, V-224882, V-224883, V-224884, V-224885, V-224886, V-224887, V-224888, V-224889, V-224890, V-224891, V-224892, V-224893, V-224894, V-224895, V-224896, V-224897, V-224898, V-224899, V-224900, V-224901, V-224902, V-224903, V-224904, V-224905, V-224906, V-224907, V-224908, V-224909, V-224910, V-224911, V-224912, V-224913, V-224914, V-224915, V-224920, V-224922, V-224924, V-224925, V-224926, V-224927, V-224928, V-224929, V-224930, V-224935, V-224936, V-224937, V-224938, V-224939, V-224940, V-224941, V-224943, V-224944, V-224945, V-224946, V-224947, V-224948, V-224949, V-224951, V-224952, V-224953, V-224955, V-224956, V-224957, V-224959, V-224960, V-224962, V-224963, V-225010, V-225013, V-225014, V-225015, V-225016, V-225017, V-225018, V-225019, V-225021, V-225022, V-225023, V-225024, V-225028, V-225029, V-225030, V-225031, V-225032, V-225033, V-225034, V-225035,

V-225038, V-225039, V-225040, V-225041, V-225042, V-225043, V-225047, V-225049, V-225050, V-225051, V-225052, V-225055, V-225056, V-225057, V-225058, V-225059, V-225061, V-225062, V-225063, V-225064, V-225065, V-225066, V-225067, V-225068, V-225069, V-225072, V-225073, V-225074, V-225076, V-225078, V-225080, V-225081, V-225082, V-225083, V-225084, V-225086, V-225087, V-225088, V-225089, V-225092, V-225093, V-236000, V-257502, V-224874, V-224932, V-224933, V-224934, V-224954, V-224958, V-224961, V-225025, V-225044, V-225045, V-225046, V-225048, V-225053, V-225054, and V-225079

Windows Server 2012 R2 MS STIG Version 3 Release 5

This release includes the following STIG settings for Windows operating systems:

V-225250, V-225318, V-225319, V-225324, V-225327, V-225328, V-225330, V-225331, V-225332, V-225333, V-225334, V-225335, V-225336, V-225342, V-225343, V-225355, V-225357, V-225358, V-225359, V-225360, V-225362, V-225363, V-225376, V-225392, V-225394, V-225412, V-225459, V-225460, V-225462, V-225468, V-225473, V-225476, V-225479, V-225480, V-225481, V-225482, V-225483, V-225484, V-225485, V-225487, V-225488, V-225489, V-225490, V-225511, V-225514, V-225525, V-225526, V-225536, V-225537, V-225239, V-225259, V-225260, V-225261, V-225263, V-225264, V-225265, V-225266, V-225267, V-225268, V-225269, V-225270, V-225271, V-225272, V-225273, V-225275, V-225276, V-225277, V-225278, V-225279, V-225280, V-225281, V-225282, V-225283, V-225284, V-225285, V-225286, V-225287, V-225288, V-225289, V-225290, V-225291, V-225292, V-225293, V-225294, V-225295, V-225296, V-225297, V-225298, V-225299, V-225300, V-225301, V-225302, V-225303, V-225304, V-225305, V-225314, V-225315, V-225316, V-225317, V-225325, V-225326, V-225329, V-225337, V-225338, V-225339, V-225340, V-225341, V-225344, V-225345, V-225346, V-225347, V-225348, V-225349, V-225350, V-225351, V-225352, V-225353, V-225356, V-225367, V-225368, V-225369, V-225370, V-225371, V-225372, V-225373, V-225374, V-225375, V-225377, V-225378, V-225379, V-225380, V-225381, V-225382, V-225383, V-225384, V-225385, V-225386, V-225389, V-225391, V-225393, V-225395, V-225397, V-225398, V-225400, V-225401, V-225402, V-225404, V-225405, V-225406, V-225407, V-225408, V-225409, V-225410, V-225411, V-225413, V-225414, V-225415, V-225441, V-225442, V-225443, V-225448, V-225452, V-225453, V-225454, V-225455, V-225456, V-225457, V-225458, V-225461, V-225463, V-225464, V-225469, V-225470, V-225471, V-225472, V-225474, V-225475, V-225477, V-225478, V-225486, V-225494, V-225500, V-225501, V-225502, V-225503, V-225504, V-225506, V-225508, V-225509, V-225510, V-225513, V-225515, V-225516, V-225517, V-225518, V-225519, V-225520, V-225521, V-225522, V-225523,

V-225524, V-225527, V-225528, V-225529, V-225530, V-225531, V-225532, V-225533, V-225534, V-225535, V-225538, V-225539, V-225540, V-225541, V-225542, V-225543, V-225544, V-225545, V-225546, V-225548, V-225549, V-225550, V-225551, V-225553, V-225554, V-225555, V-225557, V-225558, V-225559, V-225560, V-225561, V-225562, V-225563, V-225564, V-225565, V-225566, V-225567, V-225568, V-225569, V-225570, V-225571, V-225572, V-225573, V-225574, V-225274, V-225354, V-225364, V-225365, V-225366, V-225390, V-225396, V-225399, V-225444, V-225449, V-225491, V-225492, V-225493, V-225496, V-225497, V-225498, V-225505, V-225507, V-225547, V-225552, and V-225556

Microsoft .NET Framework 4.0 STIG Version 2 Release 6

The following list contains STIG settings that apply to Windows operating system components for STIG Hardened EC2 AMIs. The following list contains STIG settings that apply for STIG Hardened Windows AMIs. Not all settings apply in all cases. For example, some STIG settings might not apply to standalone servers. Organization-specific policies can also affect which settings apply, such as a requirement for administrators to review document settings.

For a complete list of Windows STIGs, see the STIGs Document Library. For information about how to view the complete list, see STIG Viewing Tools.

.NET Framework on Windows Server 2019, 2016, and 2012 R2 MS

V-225238

WindowsFirewall STIG Version 2 Release 2

The following list contains STIG settings that apply to Windows operating system components for STIG Hardened EC2 AMIs. The following list contains STIG settings that apply for STIG Hardened Windows AMIs. Not all settings apply in all cases. For example, some STIG settings might not apply to standalone servers. Organization-specific policies can also affect which settings apply, such as a requirement for administrators to review document settings.

For a complete list of Windows STIGs, see the STIGs Document Library. For information about how to view the complete list, see STIG Viewing Tools.

WindowsFirewall on Windows Server 2022, 2019, 2016, and 2012 R2 MS

V-241994, V-241995, V-241996, V-241999, V-242000, V-242001, V-242006, V-242007, V-242008, V-241989, V-241990, V-241991, V-241993, V-241998, V-242003, V-241992, V-241997, and V-242002

Internet Explorer (IE) 11 STIG Version 2 Release 5

The following list contains STIG settings that apply to Windows operating system components for STIG Hardened EC2 AMIs. The following list contains STIG settings that apply for STIG Hardened Windows AMIs. Not all settings apply in all cases. For example, some STIG settings might not apply to standalone servers. Organization-specific policies can also affect which settings apply, such as a requirement for administrators to review document settings.

For a complete list of Windows STIGs, see the STIGs Document Library. For information about how to view the complete list, see STIG Viewing Tools.

IE 11 on Windows Server 2022, 2019, 2016, and 2012 R2 MS

V-223016, V-223056, V-223078, V-223015, V-223017, V-223018, V-223019, V-223020, V-223021, V-223022, V-223023, V-223024, V-223025, V-223026, V-223027, V-223028, V-223029, V-223030, V-223031, V-223032, V-223033, V-223034, V-223035, V-223036, V-223037, V-223038, V-223039, V-223040, V-223041, V-223042, V-223043, V-223044, V-223045, V-223046, V-223048, V-223049, V-223050, V-223051, V-223052, V-223053, V-223054, V-223055, V-223057, V-223058, V-223059, V-223060, V-223061, V-223062, V-223063, V-223064, V-223065, V-223066, V-223067, V-223068, V-223069, V-223070, V-223071, V-223072, V-223073, V-223074, V-223075, V-223076, V-223077, V-223079, V-223080, V-223081, V-223082, V-223083, V-223084, V-223085, V-223086, V-223087, V-223088, V-223089, V-223090, V-223091, V-223092, V-223093, V-223094, V-223095, V-223096, V-223097, V-223098, V-223099, V-223100, V-223101, V-223102, V-223103, V-223104, V-223105, V-223106, V-223107, V-223108, V-223109, V-223110, V-223111, V-223112, V-223113, V-223114, V-223115, V-223116, V-223117, V-223118, V-223119, V-223120, V-223121, V-223122, V-223123, V-223124, V-223125, V-223126, V-223127, V-223128, V-223129, V-223130, V-223131, V-223132, V-223133, V-223134, V-223135, V-223136, V-223137, V-223138, V-223139, V-223140, V-223141, V-223142, V-223143, V-223144, V-223145, V-223146, V-223147, V-223148, V-223149, V-250540, V-250541, and V-252910

Microsoft Edge STIG Version 2 Release 2

The following list contains STIG settings that apply to Windows operating system components for STIG Hardened EC2 AMIs. The following list contains STIG settings that apply for STIG Hardened Windows AMIs. Not all settings apply in all cases. For example, some STIG settings might not apply to standalone servers. Organization-specific policies can also affect which settings apply, such as a requirement for administrators to review document settings.

For a complete list of Windows STIGs, see the STIGs Document Library. For information about how to view the complete list, see STIG Viewing Tools.

Microsoft Edge on Windows Server 2022

V-235727, V-235731, V-235751, V-235752, V-235765, V-235720, V-235721, V-235723, V-235724, V-235725, V-235726, V-235728, V-235729, V-235730, V-235732, V-235733, V-235734, V-235735, V-235736, V-235737, V-235738, V-235739, V-235740, V-235741, V-235742, V-235743, V-235744, V-235745, V-235746, V-235747, V-235748, V-235749, V-235750, V-235754, V-235756, V-235760, V-235761, V-235763, V-235764, V-235766, V-235767, V-235768, V-235769, V-235770, V-235771, V-235772, V-235773, V-235774, V-246736, V-235758, and V-235759

Microsoft Defender STIG Version 2 Release 4

The following list contains STIG settings that apply to Windows operating system components for STIG Hardened EC2 AMIs. The following list contains STIG settings that apply for STIG Hardened Windows AMIs. Not all settings apply in all cases. For example, some STIG settings might not apply to standalone servers. Organization-specific policies can also affect which settings apply, such as a requirement for administrators to review document settings.

For a complete list of Windows STIGs, see the STIGs Document Library. For information about how to view the complete list, see STIG Viewing Tools.

Microsoft Defender on Windows Server 2022

V-213427, V-213429, V-213430, V-213431, V-213432, V-213433, V-213434, V-213435, V-213436, V-213437, V-213438, V-213439, V-213440, V-213441, V-213442, V-213443, V-213444, V-213445, V-213446, V-213447, V-213448, V-213449, V-213450, V-213451, V-213455, V-213464, V-213465, V-213466, V-213426, V-213452, and V-213453

Version history

The following table provides version history updates for STIG settings that are applied to Windowsoperating systems and Windowscomponents.

Date	AMIs	Details
06/19/2025	Windows Server 2022 STIG Version 2 Release 4 Windows Server 2019 STIG Version 3 Release 4 Windows Server 2016 STIG Version 2 Release 10 Windows Server 2012 R2 MS STIG Version 3 Release 5 Microsoft .NET Framework 4.0 STIG Version 2 Release 6 WindowsFirewall STIG Version 2 Release 2 Internet Explorer 11 STIG Version 2 Release 5 Microsoft Edge STIG Version 2 Release 2 Microsoft Defender STIG Version 2 Release 4	AMIs released for 2025 Q1 and Q2 with updated versions where applicable, and applied STIGs.
03/06/2025	Windows Server 2022 STIG Version 2 Release 2 Windows Server 2019 STIG Version 3 Release 2 Windows Server 2016 STIG Version 2 Release 9 Windows Server 2012 R2 MS STIG Version 3 Release 5	AMIs released for 2024 Q4 with updated versions where applicable, and applied STIGs.

Date	AMIs	Details
	Microsoft .NET Framework 4.0 STIG Version 2 Release 2 WindowsFirewall STIG Version 2 Release 2 Internet Explorer 11 STIG Version 2 Release 5 Microsoft Edge STIG Version 2 Release 2 Microsoft Defender STIG Version 2 Release 4	
04/24/2023	Windows Server 2022 STIG Version 1 Release 1 Microsoft Edge STIG Version 1 Release 6 Microsoft Defender STIG Version 2 Release 4	Added support for Windows Server 2022, Microsoft Edge, and Microsoft Defender.
03/01/2023	Windows Server 2019 STIG Version 2 Release 5 Windows Server 2016 STIG Version 2 Release 5 Windows Server 2012 R2 MS STIG Version 3 Release 5 Microsoft .NET Framework 4.0 STIG Version 2 Release 2 WindowsFirewall STIG Version 2 Release 1 Internet Explorer 11 STIG Version 2 Release 3	AMIs released for 2022 Q4 with updated versions where applicable, and applied STIGs.

Date	AMIs	Details
07/21/202	Windows Server 2019 STIG Version 2 R4 Windows Server 2016 STIG Version 2 R4 Windows Server 2012 R2 MS STIG Version 3 R3 Microsoft .NET Framework 4.0 STIG Version 2 R1 WindowsFirewall STIG Version 2 R1 Internet Explorer 11 STIG V1 R19	AMIs released with updated versions where applicable, and applied STIGs.
12/15/201	Windows Server 2019 STIG Version 2 R3 Windows Server 2016 STIG Version 2 R3 Windows Server 2012 R2 STIG Version 3 R3 Microsoft .NET Framework 4.0 STIG Version 2 R1 WindowsFirewall STIG Version 2 R1 Internet Explorer 11 STIG V1 R19	AMIs released with updated versions where applicable, and applied STIGs.

Date	AMIs	Details
6/9/2021	Windows Server 2019 STIG Version 2 R2 Windows Server 2016 STIG Version 2 R2 Windows Server 2012 R2 STIG Version 3 R2 Microsoft .NET Framework 4.0 STIG Version 2 R1 WindowsFirewall STIG V1 R7 Internet Explorer 11 STIG V1 R19	Updated versions where applicable, and applied STIGs.
4/5/2021	Windows Server 2019 STIG Version 2 R 1 Windows Server 2016 STIG Version 2 R 1 Windows Server 2012 R2 STIG Version 3 R 1 Microsoft .NET Framework 4.0 STIG Version 2 R 1 WindowsFirewall STIG V1 R 7 Internet Explorer 11 STIG V1 R 19	Updated versions where applicable, and applied STIGs.

Date	AMIs	Details
9/18/202	Windows Server 2019 STIG V1 R 5 Windows Server 2016 STIG V1 R 12 Windows Server 2012 R2 STIG Version 2 R 19 Internet Explorer 11 STIG V1 R 19 Microsoft .NET Framework 4.0 STIG V1 R 9 WindowsFirewall STIG V1 R 7	Updated versions and applied STIGs.
12/6/201	Server 2012 R2 Core and Base V2 R17 Server 2016 Core and Base V1 R11 Internet Explorer 11 V1 R18 Microsoft .NET Framework 4.0 V1 R9 WindowsFirewall STIG V1 R17	Updated versions and applied STIGs.
9/17/201	Server 2012 R2 Core and Base V2 R16 Server 2016 Core and Base V1 R9 Server 2019 Core and Base V1 R2 Internet Explorer 11 V1 R17 Microsoft .NET Framework 4.0 V1 R8	Initial release.

AWS Windows Server NitroTPM enabled AMIs

Amazon creates a set of AMIs that are pre-configured with NitroTPM and UEFI Secure Boot requirements, as follows:

- The TPM 2.0 Command Response Buffer (CRB) driver is installed
- NitroTPM is enabled
- UEFI Secure Boot mode is enabled with Microsoft keys

For more detailed information about NitroTPM, see NitroTPM for Amazon EC2 instances in the *Amazon EC2 User Guide*.

Find Windows Server AMIs configured with NitroTPM and UEFI Secure Boot

AWS managed AMIs always include the AMI creation date as part of the name. The best way to ensure that your search returns the AMIs that you're looking for is to add date filtering for the name. Use one of the following command line options to find an AMI.

AWS CLI

Find the latest NitroTPM and UEFI Secure Boot AMIs

The following example retrieves a list of the latest Windows Server AMIs that are configured for NitroTPM and UEFI Secure Boot.

```
aws ssm get-parameters-by-path \
    --path "/aws/service/ami-windows-latest" \
    --recursive \
    --query 'Parameters[*].{Name:Name,Value:Value}' \
    --output text | grep "TPM-Windows_Server" | sort
```

Find a specific AMI

The following example retrieves Windows Server AMIs that are configured for NitroTPM and UEFI Secure Boot by filtering on the AMI name, the owner, the platform, and the creation date (year and month). Output is formatted as a table with columns for the AMI name and image ID.

```
aws ec2 describe-images \
    --owners amazon \
    --filters \
        "Name=name,Values=TPM-Windows_Server-*" \
        "Name=platform,Values=windows" \
        "Name=creation-date,Values=2025-05*" \
    --query 'Images[].[Name,ImageId]' \
```

```
    --output text | sort
```

PowerShell (recommended)

Find the latest NitroTPM and UEFI Secure Boot AMIs

The following example retrieves a list of the latest Windows Server AMIs that are configured for NitroTPM and UEFI Secure Boot.

```
Get-SSMLatestEC2Image `
    -Path ami-windows-latest `
    -ImageName TPM-Windows_Server-* | `
Sort-Object Name
```

> **Note**
>
> If this command doesn't run in your environment, you might be missing a PowerShell module. For more information about this command, see Get-SSMLatestEC2Image Cmdlet.
> Alternatively, you can use the CloudShell console and run pwsh to bring up a PowerShell prompt that already has all of the AWS tools installed. For more information, see the AWS CloudShell User Guide.

Find a specific AMI

The following example retrieves Windows Server AMIs that are configured for NitroTPM and UEFI Secure Boot by filtering on the AMI name, the owner, the platform, and the creation date (year and month). Output is formatted as a table with columns for the AMI name and image ID.

```
Get-EC2Image `
    -Owner amazon `
    -Filter @(
        @{Name = "name"; Values = @("TPM-Windows_Server-*")},
        @{Name = "owner-alias"; Values = @("amazon")},
        @{Name = "platform"; Values = "windows"},
        @{Name = "creation-date"; Values = @("2025-05*")}
    ) | `
Sort-Object Name |`
Format-Table Name, ImageID -AutoSize
```

How Amazon creates AWS Windows AMIs

The following content is a high level overview of the process Amazon uses to create AWS Windows AMIs. Details include what you can expect from an official AWS Windows AMI, as well as the standards that Amazon uses to validate AMI security and reliability.

Where AWS gets the Windows Server installation media

When a new version of Windows Server is released, we download the Windows ISO from Microsoft and validate the hash Microsoft publishes. An initial AMI is then created from the Windows distribution ISO. The drivers needed to boot on EC2 are included in addition to our EC2 launch agent. To prepare this initial AMI for public release, we perform automated processes to convert the ISO to an AMI. This prepared AMI is used for the monthly automated update and release process.

What to expect from an official AWS Windows AMI

Amazon provides AWS Windows AMIs with a variety of configurations for popular versions of Microsoft supported Windows Server Operating Systems. As outlined in the previous section, we start with the Windows Server ISO from Microsoft's Volume Licensing Service Center (VLSC) and validate the hash to ensure it matches Microsoft's documentation for new Windows Server operating systems.

We perform the following changes using automation on AWS to take the current Windows Server AMIs and update them:

- Install all Microsoft recommended Windows security patches. We release images shortly after the monthly Microsoft patches are made available.
- Install the latest drivers for AWS hardware, including network and disk drivers, the EC2WinUtil utility for troubleshooting, as well as GPU drivers in selected AMIs.
- Include the following AWS launch agent software by default:
  - EC2Launch v2 for Windows Server 2022 and 2025, and optionally for Windows Server 2019 and 2016 with specific AMIs.
  - EC2Launch v1 for Windows Server 2016 and 2019.
  - EC2Config for Windows Server 2012 R2 and earlier.
- Configure Windows Time to use the Amazon Time Sync Service.
- Change all power schemes to set the display to never turn off.

- Perform minor bug fixes – generally one-line registry changes to enable or disable features that we have found to improve performance on AWS.
- Tests and validates AMIs across new and existing EC2 platforms to help ensure compatibility, stability, and consistency before release.

For a more detailed list that includes initialization, installation, and configuration settings that are applied, see Updates applied for AWS Windows AMIs.

How Amazon validates security, integrity, and authenticity of software on AMIs

We take a number of steps during the image build process, to maintain the security, integrity, and authenticity of AWS Windows AMIs. A few examples include:

- AWS Windows AMIs are built using source media obtained directly from Microsoft.
- Windows Updates are downloaded directly from Microsoft's Windows Update Service by Windows, and installed on the instance used to create the AMI during the image build process.
- AWS Software is downloaded from secure S3 buckets and installed in the AMIs.
- Drivers, such as for the chipset and GPU, are obtained directly from the vendor, stored in secure S3 buckets, and installed on the AMIs during the image build process.

How Amazon decides which AWS Windows AMIs to offer

Each AMI is extensively tested prior to release to the public. We periodically streamline our AMI offerings to simplify customer choice and to reduce costs.

- New AMI offerings are created for new OS releases. You can count on Amazon releasing *Base*, *Core*, and *SQL Express/Standard/Web/Enterprise* offerings in English and other widely used languages. The primary difference between Base and Core offerings is that Base offerings have a desktop/GUI whereas Core offerings are PowerShell command line only. For more information, see Windows Server Core on the Microsoft website.
- New AMI offerings are created to support new platforms – for example, the Deep Learning andNvidia AMIs were created to support customers using our GPU-based instance types (P2 and P3, G3, and others).
- Less popular AMIs are sometimes removed. If we see a particular AMI is launched only a few times in its entire lifespan, we will remove it in favor of more widely used options.

If there is an AMI variant that you would like to see, let us know by opening a support case, or by providing feedback.

Patches, security updates, and AMI IDs

Amazon provides updated, fully-patched AWS Windows AMIs within five business days of Microsoft's patch Tuesday (the second Tuesday of each month). The new AMIs are available immediately from the **Images** page in the Amazon EC2 console. The new AMIs are available in the AWS Marketplace and the **Quick Start** tab of the launch instance wizard within a few days of their release.

> **Note**
>
> Instances launched from Windows Server 2019 and later AMIs may show a Windows Update dialog message stating "Some settings are managed by your organization." This message appears as a result of changes in Windows Server 2019 and does not impact the behavior of Windows Update or your ability to manage update settings.
> To remove this warning, see "Some settings are managed by your organization".

AWS Windows AMIs are publicly available for three months after they are released. Within 10 days after the release of new AMIs, AWS changes access for AMIs that are more than three months old to make them private.

After AWS makes an AMI private, you may no longer retrieve it by any method. In the console, the **AMI ID** field for a private AMI states, `Cannot load detail for ami-1234567890abcdef0. You may not be permitted to view it.`

If an AMI is deprecated but is not yet marked private, you can still use it. However, we recommend that you always use the latest version.

The AWS Windows AMIs; in each release have new AMI IDs. Therefore, we recommend that you write scripts that locate the latest AWS Windows AMIs by their names, rather than by their IDs. For more information, see the following examples:

- Get-EC2ImageByName (AWS Tools for Windows PowerShell)
- Query for the Latest AWS Windows AMI Using Systems Manager Parameter Store
- Walkthrough: Looking Up Amazon Machine Image IDs (AWS Lambda, AWS CloudFormation)

Ports and Protocols for AWS Windows AMIs

The following tables list the ports, protocols, and directions by workload for AWS Windows Amazon Machine Images (AMIs).

Contents

AllJoyn Router

OS	Rule	Description	Port	Protocol	Direction
Windows Server 2016 Windows Server 2019	AllJoyn Router (TCP-In)	Inbound rule for AllJoyn Router traffic [TCP]	Local: 9955 Remote: Any	TCP	In

OS	Rule	Description	Port	Protocol	Direction
Windows Server 2022	AllJoyn Router (TCP-Out)	Outbound rule for AllJoyn Router traffic [TCP]	Local: Any Remote: Any	TCP	Out
	AllJoyn Router (UDP-In)	Inbound rule for AllJoyn Router traffic [UDP]	Local: Any Remote: Any	UDP	In
	AllJoyn Router (UDP-Out)	Outbound rule for AllJoyn Router traffic [UDP]	Local: Any Remote: Any	UDP	Out

Cast to Device

OS	Rule	Description	Port	Protocol	Direction
Windows Server 2016 Windows Server 2019 Windows Server 2022	Cast to Device functionality (qWave-TCP-In)	Inbound rule for the Cast to Device functionality to allow use of the Quality Windows Audio Video Experience Service. [TCP 2177]	Local: 2177 Remote: Any	TCP	In

OS	Rule	Description	Port	Protocol	Direction
	Cast to Device functionality (qWave-TCP-Out)	Outbound rule for the Cast to Device functionality to allow use of the Quality Windows Audio Video Experience Service. [TCP 2177]	Local: Any Remote: 2177	TCP	Out
	Cast to Device functionality (qWave-UDP-In)	Inbound rule for the Cast to Device functionality to allow use of the Quality Windows Audio Video Experience Service. [UDP 2177]	Local: 2177 Remote: Any	UDP	In

OS	Rule	Description	Port	Protocol	Direction
	Cast to Device functionality (qWave-UDP-Out)	Outbound rule for the Cast to Device functionality to allow use of the Quality Windows Audio Video Experience Service. [UDP 2177]	Local: Any Remote: 2177	UDP	Out
	Cast to Device SSDP Discovery (UDP-In)	Inbound rule to allow discovery of Cast to Device targets using SSDP	Local: Ply2Disc Remote: Any	UDP	In
	Cast to Device Streaming Server (HTTP-Streaming-In)	Inbound rule for the Cast to Device server to allow streaming using HTTP. [TCP 10246]	Local: 10246 Remote: Any	TCP	In

OS	Rule	Description	Port	Protocol	Direction
	Cast to Device Streaming Server (RTCP-Streaming-In)	Inbound rule for the Cast to Device server to allow streaming using RTSP and RTP. [UDP]	Local: Any Remote: Any	UDP	In
	Cast to Device Streaming Server (RTP-Streaming-Out)	Outbound rule for the Cast to Device server to allow streaming using RTSP and RTP. [UDP]	Local: Any Remote: Any	UDP	Out
	Cast to Device Streaming Server (RTSP-Streaming-In)	Inbound rule for the Cast to Device server to allow streaming using RTSP and RTP. [TCP 23554, 23555, 23556]	Local: 235, 542, 355, 523, 556 Remote: Any	TCP	In

OS	Rule	Description	Port	Protocol	Direction
	Cast to Device UPnP Events (TCP-In)	Inbound rule to allow receiving UPnP Events from Cast to Device targets	Local: 2869 Remote: Any	TCP	In

Core Networking

Windows Server 2016, 2019, and 2022

OS	Rule	Definition	Port	Protocol	Direction
Windows Server 2016 Windows Server 2019 Windows Server 2022	Destination Unreachable (ICMPv6-In)	Destination Unreachable error messages are sent from any node that a packet traverses which is unable to forward the packet for any reason except congestion.		ICMPv6	In
	Destination Unreachable Fragmenta	Destination Unreachable Fragmenta		ICMPv4	In

OS	Rule	Definition	Port	Protocol	Direction
	tion Needed (ICMPv4-In)	tion Needed error me ssages are sent from any node that a packet traverses which is unable to forward the packet because fragmenta tion was needed and the don't fragment bit was set.			

OS	Rule	Definition	Port	Protocol	Direction
	Core Networking - DNS (UDP-Out)	Outbound rule to allow DNS requests. DNS responses based on requests that match this rule are permitted regardless of source address. This behavior is classified as loose source mapping.	Local: Any Remote: 53	UDP	Out
	Dynamic Host Configuration Protocol (DHCP-In)	Allows DHCP (Dynamic Host Configuration Protocol) messages for stateful auto-configuration.	Local: 68 Remote: 67	UDP	In

OS	Rule	Definition	Port	Protocol	Direction
	Dynamic Host Configuration Protocol (DHCP-Out)	Allows DHCP (Dynamic Host Configuration Protocol) messages for stateful auto-configuration.	Local: 68 Remote: 67	UDP	Out
	Dynamic Host Configuration Protocol for IPv6 (DHCPV6-In)	Allows DHCPV6 (Dynamic Host Configuration Protocol for IPv6) messages for stateful and stateless configuration.	Local: 546 Remote: 547	UDP	In

OS	Rule	Definition	Port	Protocol	Direction
	Dynamic Host Configuration Protocol for IPv6 (DHCPV6-Out)	Allows DHCPV6 (Dynamic Host Configuration Protocol for IPv6) messages for stateful and stateless configuration.	Local: 546 Remote: 547	UDP	Out
	Core Networking - Group Policy (LSASS-Out)	Outbound rule to allow remote LSASS traffic for Group Policy updates.	Local: Any Remote: Any	TCP	Out
	Core Networking - Group Policy (NP-Out)	Core Networking - Group Policy (NP-Out)	Local: Any Remote: 445	TCP	Out
	Core Networking - Group Policy (TCP-Out)	Outbound rule to allow remote RPC traffic for Group Policy updates.	Local: Any Remote: Any	TCP	Out

OS	Rule	Definition	Port	Protocol	Direction
	Internet Group Management Protocol (IGMP-In)	IGMP messages are sent and received by nodes to create, join, and depart multicast groups.		2	In
	Core Networking - Internet Group Management Protocol (IGMP-Out)	IGMP messages are sent and received by nodes to create, join, and depart multicast groups.		2	Out
	Core Networking - IPHTTPS (TCP-In)	Inbound TCP rule to allow IPHTTPS tunneling technology to provide connectivity across HTTP proxies and firewalls.	Local: IPHTPS Remote: Any	TCP	In

OS	Rule	Definition	Port	Protocol	Direction
	Core Networking - IPHTTPS (TCP-Out)	Outbound TCP rule to allow IPHTTPS tunneling technology to provide connectivity across HTTP proxies and firewalls.	Local: Any Remote: IPHTPS	TCP	Out
	IPv6 (IPv6-In)	Inbound rule required to permit IPv6 traffic for ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) and 6to4 tunneling services.		41	In

OS	Rule	Definition	Port	Protocol	Direction
	IPv6 (IPv6-Out)	Outbound rule required to permit IPv6 traffic for ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) and 6to4 tunneling services.		41	Out
	Multicast Listener Done (ICMPv6-In)	Multicast Listener Done messages inform local routers that there are no longer any members remaining for a specific multicast address on the subnet.		ICMPv6	In

OS	Rule	Definition	Port	Protocol	Direction
	Multicast Listener Done (ICMPv6-Out)	Multicast Listener Done messages inform local routers that there are no longer any members remaining for a specific multicast address on the subnet.		ICMPv6	Out
	Multicast Listener Query (ICMPv6-In)	An IPv6 multicast-capable router uses the Multicast Listener Query message to query a link for multicast group membership.		ICMPv6	In

OS	Rule	Definition	Port	Protocol	Direction
	Multicast Listener Query (ICMPv6-Out)	An IPv6 multicast-capable router uses the Multicast Listener Query message to query a link for multicast group membership.		ICMPv6	Out

OS	Rule	Definition	Port	Protocol	Direction
	Multicast Listener Report (ICMPv6-In)	The Multicast Listener Report message is used by a listening node to either immediately report its interest in receiving multicast traffic at a specific multicast address or in response to a Multicast Listener Query.		ICMPv6	In

OS	Rule	Definition	Port	Protocol	Direction
	Multicast Listener Report (ICMPv6-Out)	The Multicast Listener Report message is used by a listening node to either immediately report its interest in receiving multicast traffic at a specific multicast address or in response to a Multicast Listener Query.		ICMPv6	Out

OS	Rule	Definition	Port	Protocol	Direction
	Multicast Listener Report v2 (ICMPv6-In)	Multicast Listener Report v2 message is used by a listening node to either immediately report its interest in receiving multicast traffic at a specific multicast address or in response to a Multicast Listener Query.		ICMPv6	In

OS	Rule	Definition	Port	Protocol	Direction
	Multicast Listener Report v2 (ICMPv6-Out)	Multicast Listener Report v2 message is used by a listening node to either immediately report its interest in receiving multicast traffic at a specific multicast address or in response to a Multicast Listener Query.		ICMPv6	Out

OS	Rule	Definition	Port	Protocol	Direction
	Neighbor Discovery Advertisement (ICMPv6-In)	Neighbor Discovery Advertisement messages are sent by nodes to notify other nodes of link-layer address changes or in response to a Neighbor Discovery Solicitation request.		ICMPv6	In

OS	Rule	Definition	Port	Protocol	Direction
	Neighbor Discovery Advertisement (ICMPv6-Out)	Neighbor Discovery Advertisement messages are sent by nodes to notify other nodes of link-layer address changes or in response to a Neighbor Discovery Solicitation request.		ICMPv6	Out
	Neighbor Discovery Solicitation (ICMPv6-In)	Neighbor Discovery Solicitations are sent by nodes to discover the link-layer address of another on-link IPv6 node.		ICMPv6	In

OS	Rule	Definition	Port	Protocol	Direction
	Neighbor Discovery Solicitation (ICMPv6-Out)	Neighbor Discovery Solicitations are sent by nodes to discover the link-layer address of another on-link IPv6 node.		ICMPv6	Out
	Packet Too Big (ICMPv6-In)	Packet Too Big error messages are sent from any node that a packet traverses which is unable to forward the packet because the packet is too large for the next link.		ICMPv6	In

OS	Rule	Definition	Port	Protocol	Direction
	Packet Too Big (ICMPv6-Out)	Packet Too Big error messages are sent from any node that a packet traverses which is unable to forward the packet b ecause the packet is too large for the next link.		ICMPv6	Out
	Parameter Problem (ICMPv6-In)	Parameter Problem error messages are sent by nodes when packets are incorrectly generated.		ICMPv6	In

OS	Rule	Definition	Port	Protocol	Direction
	Parameter Problem (ICMPv6-Out)	Parameter Problem error messages are sent by nodes when packets are incorrectly generated.		ICMPv6	Out
	Router Advertisement (ICMPv6-In)	Router Advertisement messages are sent by routers to other nodes for stateless auto-configuration.		ICMPv6	In
	Router Advertisement (ICMPv6-Out)	Router Advertisement messages are sent by routers to other nodes for stateless auto-configuration.		ICMPv6	Out

OS	Rule	Definition	Port	Protocol	Direction
	Router Solicitation (ICMPv6-In)	Router Solicitation messages are sent by nodes seeking routers to provide stateless auto-conf iguration.		ICMPv6	In
	Router Solicitation (ICMPv6-O ut)	Router Solicitation messages are sent by nodes seeking routers to provide stateless auto-conf iguration.		ICMPv6	Out

OS	Rule	Definition	Port	Protocol	Direction
	Core Networking - Teredo (UDP-In)	Inbound UDP rule to allow Teredo edge traversal. This technology provides address assignment and automatic tunneling for unicast IPv6 traffic when an IPv6/IPv4 host is located behind an IPv4 network address translator.	Local: Teredo Remote: Any	UDP	In

OS	Rule	Definition	Port	Protocol	Direction
	Core Networking - Teredo (UDP-Out)	Outbound UDP rule to allow Teredo edge traversal. This technology provides address assignment and automatic tunneling for unicast IPv6 traffic when an IPv6/IPv4 host is located behind an IPv4 network address translator.	Local: Any Remote: Any	UDP	Out

OS	Rule	Definition	Port	Protocol	Direction
	Time Exceeded (ICMPv6-In)	Time Exceeded error messages are generated from any node tha t a packet traverses if the Hop Limit value is decre mented to zero at any point on the path.		ICMPv6	In

OS	Rule	Definition	Port	Protocol	Direction
	Time Exceeded (ICMPv6-Out)	Time Exceeded error messages are generated from any node that a packet traverses if the Hop Limit value is decremented to zero at any point on the path.		ICMPv6	Out

Windows Server 2012 and 2012 R2

OS	Rule	Definition	Port	Protocol	Direction
Windows Server 2012 Windows Server 2012 R2	Destination Unreachable (ICMPv6-In)	Destination Unreachable error messages are sent from any node that a packet traverses which is unable to forward the	Local: 68 Remote: 67	ICMPv6	In

OS	Rule	Definition	Port	Protocol	Direction
		packet for any reason except congestion.			
	Destination Unreachable Fragmentation Needed (ICMPv4-In)	Destination Unreachable Fragmentation Needed error messages are sent from any node that a packet traverses which is unable to forward the packet because fragmentation was needed and the don't fragment bit was set.	Local: 68 Remote: 67	ICMPv4	In

OS	Rule	Definition	Port	Protocol	Direction
	Core Networking - DNS (UDP-Out)	Outbound rule to allow DNS requests. DNS responses based on requests that match this rule are permitted regardless of source address. This behavior is classified as loose source mapping.	Local: Any Remote: 53	UDP	Out
	Dynamic Host Configuration Protocol (DHCP-In)	Allows DHCP (Dynamic Host Configuration Protocol) messages for stateful auto-configuration.	Local: 68 Remote: 67	UDP	In

OS	Rule	Definition	Port	Protocol	Direction
	Dynamic Host Configuration Protocol (DHCP-Out)	Allows DHCP (Dynamic Host Configuration Protocol) messages for stateful auto-configuration.	Local: 68 Remote: 67	UDP	Out
	Dynamic Host Configuration Protocol for IPv6 (DHCPV6-In)	Allows DHCPV6 (Dynamic Host Configuration Protocol for IPv6) messages for stateful and stateless configuration.	Local: 546 Remote: 547	UDP	In

OS	Rule	Definition	Port	Protocol	Direction
	Dynamic Host Configuration Protocol for IPv6 (DHCPV6-Out)	Allows DHCPV6 (Dynamic Host Configuration Protocol for IPv6) messages for stateful and stateless configuration.	Local: 546 Remote: 547	UDP	Out
	Core Networking - Group Policy (LSASS-Out)	Outbound rule to allow remote LSASS traffic for Group Policy updates.	Local: Any Remote: Any	TCP	Out
	Core Networking - Group Policy (NP-Out)	Core Networking - Group Policy (NP-Out)	Local: Any Remote: 445	TCP	Out
	Core Networking - Group Policy (TCP-Out)	Outbound rule to allow remote RPC traffic for Group Policy updates.	Local: Any Remote: Any	TCP	Out

OS	Rule	Definition	Port	Protocol	Direction
	Internet Group Management Protocol (IGMP-In)	IGMP messages are sent and received by nodes to create, join, and depart multicast groups.	Local: 68 Remote: 67	2	In
	Core Networking - Internet Group Management Protocol (IGMP-Out)	IGMP messages are sent and received by nodes to create, join, and depart multicast groups.	Local: 68 Remote: 67	2	Out
	Core Networking - IPHTTPS (TCP-In)	Inbound TCP rule to allow IPHTTPS tunneling technology to provide connectivity across HTTP proxies and firewalls.	Local: IPHTPS Remote: Any	TCP	In

OS	Rule	Definition	Port	Protocol	Direction
	Core Networking - IPHTTPS (TCP-Out)	Outbound TCP rule to allow IPHTTPS tunneling technology to provide connectivity across HTTP proxies and firewalls.	Local: Any Remote: IPHTPS	TCP	Out
	IPv6 (IPv6-In)	Inbound rule required to permit IPv6 traffic for ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) and 6to4 tunneling services.	Local: Any Remote: 445	41	In

OS	Rule	Definition	Port	Protocol	Direction
	IPv6 (IPv6-Out)	Outbound rule required to permit IPv6 traffic for ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) and 6to4 tunneling services.	Local: Any Remote: 445	41	Out
	Multicast Listener Done (ICMPv6-In)	Multicast Listener Done messages inform local routers that there are no longer any members remaining for a specific multicast address on the subnet.	Local: 68 Remote: 67	ICMPv6	In

OS	Rule	Definition	Port	Protocol	Direction
	Multicast Listener Done (ICMPv6-Out)	Multicast Listener Done messages inform local routers that there are no longer any members remaining for a specific multicast address on the subnet.	Local: 68 Remote: 67	ICMPv6	Out
	Multicast Listener Query (ICMPv6-In)	An IPv6 multicast-capable router uses the Multicast Listener Query message to query a link for multicast group membership.	Local: 68 Remote: 67	ICMPv6	In

OS	Rule	Definition	Port	Protocol	Direction
	Multicast Listener Query (ICMPv6-Out)	An IPv6 multicast-capable router uses the Multicast Listener Query message to query a link for multicast group membership.	Local: 68 Remote: 67	ICMPv6	Out

OS	Rule	Definition	Port	Protocol	Direction
	Multicast Listener Report (ICMPv6-In)	The Multicast Listener Report message is used by a listening node to either immediately report its interest in receiving multicast traffic at a specific multicast address or in response to a Multicast Listener Query.	Local: 68 Remote: 67	ICMPv6	In

OS	Rule	Definition	Port	Protocol	Direction
	Multicast Listener Report (ICMPv6-Out)	The Multicast Listener Report message is used by a listening node to either immediately report its interest in receiving multicast traffic at a specific multicast address or in response to a Multicast Listener Query.	Local: 68 Remote: 67	ICMPv6	Out

OS	Rule	Definition	Port	Protocol	Direction
	Multicast Listener Report v2 (ICMPv6-In)	Multicast Listener Report v2 message is used by a listening node to either immediately report its interest in receiving multicast traffic at a specific multicast address or in response to a Multicast Listener Query.	Local: 68 Remote: 67	ICMPv6	In

OS	Rule	Definition	Port	Protocol	Direction
	Multicast Listener Report v2 (ICMPv6-Out)	Multicast Listener Report v2 message is used by a listening node to either immediately report its interest in receiving multicast traffic at a specific multicast address or in response to a Multicast Listener Query.	Local: 68 Remote: 67	ICMPv6	Out

OS	Rule	Definition	Port	Protocol	Direction
	Neighbor Discovery Advertisement (ICMPv6-In)	Neighbor Discovery Advertisement messages are sent by nodes to notify other nodes of link-layer address changes or in response to a Neighbor Discovery Solicitation request.	Local: 68 Remote: 67	ICMPv6	In

OS	Rule	Definition	Port	Protocol	Direction
	Neighbor Discovery Advertisement (ICMPv6-Out)	Neighbor Discovery Advertisement messages are sent by nodes to notify other nodes of link-layer address changes or in response to a Neighbor Discovery Solicitation request.	Local: 68 Remote: 67	ICMPv6	Out
	Neighbor Discovery Solicitation (ICMPv6-In)	Neighbor Discovery Solicitations are sent by nodes to discover the link-layer address of another on-link IPv6 node.	Local: 68 Remote: 67	ICMPv6	In

OS	Rule	Definition	Port	Protocol	Direction
	Neighbor Discovery Solicitation (ICMPv6-Out)	Neighbor Discovery Solicitations are sent by nodes to discover the link-layer address of another on-link IPv6 node.	Local: 68 Remote: 67	ICMPv6	Out
	Packet Too Big (ICMPv6-In)	Packet Too Big error messages are sent from any node that a packet traverses which is unable to forward the packet because the packet is too large for the next link.	Local: 68 Remote: 67	ICMPv6	In

OS	Rule	Definition	Port	Protocol	Direction
	Packet Too Big (ICMPv6-Out)	Packet Too Big error messages are sent from any node that a packet traverses which is unable to forward the packet because the packet is too large for the next link.	Local: 68 Remote: 67	ICMPv6	Out
	Parameter Problem (ICMPv6-In)	Parameter Problem error messages are sent by nodes when packets are incorrectly generated.	Local: 68 Remote: 67	ICMPv6	In

OS	Rule	Definition	Port	Protocol	Direction
	Parameter Problem (ICMPv6-Out)	Parameter Problem error messages are sent by nodes when packets are incorrectly generated.	Local: 68 Remote: 67	ICMPv6	Out
	Router Advertisement (ICMPv6-In)	Router Advertisement messages are sent by routers to other nodes for stateless auto-configuration.	Local: 68 Remote: 67	ICMPv6	In
	Router Advertisement (ICMPv6-Out)	Router Advertisement messages are sent by routers to other nodes for stateless auto-configuration.	Local: 68 Remote: 67	ICMPv6	Out

OS	Rule	Definition	Port	Protocol	Direction
	Router Solicitation (ICMPv6-In)	Router Solicitation messages are sent by nodes seeking routers to provide stateless auto-conf iguration.	Local: 68 Remote: 67	ICMPv6	In
	Router Solicitation (ICMPv6-O ut)	Router Solicitation messages are sent by nodes seeking routers to provide stateless auto-conf iguration.	Local: 68 Remote: 67	ICMPv6	Out

OS	Rule	Definition	Port	Protocol	Direction
	Core Networking - Teredo (UDP-In)	Inbound UDP rule to allow Teredo edge traversal. This technology provides address assignment and automatic tunneling for unicast IPv6 traffic when an IPv6/IPv4 host is located behind an IPv4 network address translator.	Local: Teredo Remote: Any	UDP	In

OS	Rule	Definition	Port	Protocol	Direction
	Core Networking - Teredo (UDP-Out)	Outbound UDP rule to allow Teredo edge traversal. This technology provides address assignment and automatic tunneling for unicast IPv6 traffic when an IPv6/IPv4 host is located behind an IPv4 network address translator.	Local: Any Remote: Any	UDP	Out

OS	Rule	Definition	Port	Protocol	Direction
	Time Exceeded (ICMPv6-In)	Time Exceeded error messages are generated from any node tha t a packet traverses if the Hop Limit value is decre mented to zero at any point on the path.	Local: 68 Remote: 67	ICMPv6	In

OS	Rule	Definition	Port	Protocol	Direction
	Time Exceeded (ICMPv6-Out)	Time Exceeded error messages are generated from any node that a packet traverses if the Hop Limit value is decremented to zero at any point on the path.	Local: 68 Remote: 67	ICMPv6	Out

Delivery Optimization

OS	Rule	Definition	Port	Protocol	Direction
Windows Server 2019 Windows Server 2022	DeliveryOptimization-TCP-In	Inbound rule to allow Delivery Optimization to connect to remote endpoints.	Local: 7680 Remote: Any	TCP	In
	DeliveryOptimization-UDP-In	Inbound rule to allow Delivery Optimization	Local: 7680 Remote: Any	UDP	In

OS	Rule	Definition	Port	Protocol	Direction
		to connect to remote endpoints.			

Diag Track

Windows Server 2019 and 2022

OS	Rule	Definition	Port	Protocol	Direction
Windows Server 2019 Windows Server 2022	Connected User Experiences and Telemetry	Unified Telemetry Client Outbound Traffic.	Local: Any Remote: 443	TCP	Out

Windows Server 2016

OS	Rule	Definition	Port	Protocol	Direction
Windows Server 2016	Connected User Experiences and Telemetry	Unified Telemetry Client Outbound Traffic.	Local: Any Remote: Any	TCP	Out

DIAL Protocol Server

OS	Rule	Definition	Port	Protocol	Direction
Windows Server 2016	DIAL protocol server (HTTP-In)	Inbound rule for DIAL protocol	Local: 10247	TCP	In

OS	Rule	Definition	Port	Protocol	Direction
Windows Server 2019 Windows Server 2022		server to allow remote c ontrol of Apps using HTTP.	Remote: Any		

File and Printer Sharing

OS	Rule	Definition	Port	Protocol	Direction
Windows Server 2012 Windows Server 2012 R2	File and Printer Sharing (Echo Request - ICMPv4-In)	Echo Request messages are sent as ping requests to other nodes.	Local: 5355 Remote: Any	ICMPv4	In
	File and Printer Sharing (Echo Request - ICMPv4-Out)	Echo Request messages are sent as ping requests to other nodes.	Local: 5355 Remote: Any	ICMPv4	Out
	File and Printer Sharing (Echo Request - ICMPv6-In)	Echo Request messages are sent as ping requests to other nodes.	Local: 5355 Remote: Any	ICMPv6	In
	File and Printer Sharing	Echo Request messages are sent as ping	Local: 5355	ICMPv6	Out

OS	Rule	Definition	Port	Protocol	Direction
	(Echo Request - ICMPv6-Out)	requests to other nodes.	Remote: Any		
	File and Printer Sharing (LLMNR-UDP-In)	Inbound rule for File and Printer Sharing to allow Link Local Multicast Name Resolution.	Local: 5355 Remote: Any	UDP	In
	File and Printer Sharing (LLMNR-UDP-Out)	Outbound rule for File and Printer Sharing to allow Link Local Multicast Name Resolution.	Local: Any Remote: 5355	UDP	Out
	File and Printer Sharing (NB-Datagram-In)	Inbound rule for File and Printer Sharing to allow NetBIOS Datagram transmission and reception.	Local: 138 Remote: Any	UDP	In

OS	Rule	Definition	Port	Protocol	Direction
	File and Printer Sharing (NB-Datagram-Out)	Outbound rule for File and Printer Sharing to allow NetBIOS Datagram transmission and reception.	Local: Any Remote: 138	UDP	Out
	File and Printer Sharing (NB-Name-In)	Inbound rule for File and Printer Sharing to allow NetBIOS Name Resolution.	Local: 137 Remote: Any	UDP	In
	File and Printer Sharing (NB-Name-Out)	Outbound rule for File and Printer Sharing to allow NetBIOS Name Resolution.	Local: Any Remote: 137	UDP	Out

OS	Rule	Definition	Port	Protocol	Direction
	File and Printer Sharing (NB-Session-In)	Inbound rule for File and Printer Sharing to allow NetBIOS Session Service connections.	Local: 139 Remote: Any	TCP	In
	File and Printer Sharing (NB-Session-Out)	Outbound rule for File and Printer Sharing to allow NetBIOS Session Service connections.	Local: Any Remote: 139	TCP	Out
	File and Printer Sharing (SMB-In)	Inbound rule for File and Printer Sharing to allow Server Message Block transmission and reception via Named Pipes.	Local: 445 Remote: Any	TCP	In

OS	Rule	Definition	Port	Protocol	Direction
	File and Printer Sharing (SMB-Out)	Outbound rule for File and Printer Sharing to allow Server Message Block transmission and reception via Named Pipes.	Local: Any Remote: 445	TCP	Out
	File and Printer Sharing (Spooler Service - RPC)	Inbound rule for File and Printer Sharing to allow the Print Spooler Service to communicate via TCP/RPC.	Local: RPC Remote: Any	TCP	In
	File and Printer Sharing (Spooler Service - RPC-EPMAP)	Inbound rule for the RPCSS service to allow RPC/TCP traffic for the Spooler Service.	Local: RPC-EPMap Remote: Any	TCP	In

File Server Remote Management

OS	Rule	Definition	Port	Protocol	Direction
Windows Server 2012 Windows Server 2012 R2	File Server Remote Management (DCOM-In)	Inbound rule to allow DCOM traffic to manage the File Services role.	Local: 135 Remote: Any	TCP	In
	File Server Remote Management (SMB-In)	Inbound rule to allow SMB traffic to manage the File Services role.	Local: 445 Remote: Any	TCP	In
	WMI-In	Inbound rule to allow WMI traffic to manage the File Services role.	Local: RPC Remote: Any	TCP	In

ICMP v4 All

OS	Rule	Port	Protocol	Direction
Windows Server 2012 Windows Server 2012 R2	All ICMP v4	Local: 139 Remote: Any	ICMPv4	In

Microsoft Edge

OS	Rule	Port	Protocol	Direction
Windows Server 2022	Microsoft Edge (mDNS-In)	Local: 5353 Remote: Any	UDP	In

Microsoft Media Foundation Network Source

OS	Rule	Port	Protocol	Direction
Windows Server 2022	Microsoft Media Foundation Network Source IN [TCP 554]	Local: 554, 8554-8558 Remote: Any	TCP	In
	Microsoft Media Foundatio n Network Source IN [UDP 5004-5009]	Local: 5000-5020 Remote: Any	UDP	In
	Microsoft Media Foundation Network Source OUT [TCP ALL]	Local: Any Remote: 554, 8554-8558	TCP	In

Multicast

Windows Server 2019 and 2022

OS	Rule	Definition	Port	Protocol	Direction
Windows Server 2019 Windows Server 2022	mDNS (UDP-In)	Inbound rule for mDNS traffic.	Local: 5353 Remote: Any	UDP	In
	mDNS (UDP-Out)	Outbound rule for mDNS traffic.	Local: Any Remote: 5353	UDP	Out

Windows Server 2016

OS	Rule	Definition	Port	Protocol	Direction
Windows Server 2016	mDNS (UDP-In)	Inbound rule for mDNS traffic.	Local: mDNS Remote: Any	UDP	In
	mDNS (UDP-Out)	Outbound rule for mDNS traffic.	Local: 5353 Remote: Any	UDP	Out

Remote Desktop

Windows Server 2012 R2, 2016, 2019, and 2022

OS	Rule	Definition	Port	Protocol	Direction
	Remote Desktop	Inbound rule for the	Local: Any	TCP	In

OS	Rule	Definition	Port	Protocol	Direction
Windows Server 2012 R2 Windows Server 2016 Windows Server 2019 Windows Server 2022	- Shadow (TCP-In)	Remote Desktop service to allow sh adowing of an existing Remote Desktop session.	Remote: Any		
	Remote Desktop - User Mode (TCP-In)	Inbound rule for the Remote Desktop service to allow RDP traffic.	Local: 3389 Remote: Any	TCP	In
	Remote Desktop - User Mode (UDP-In)	Inbound rule for the Remote Desktop service to allow RDP traffic.	Local: 3389 Remote: Any	UDP	In

Windows Server 2012

OS	Rule	Definition	Port	Protocol	Direction
Windows Server 2012	Remote Desktop - User Mode (TCP-In)	Inbound rule for the Remote Desktop service to	Local: 3389 Remote: Any	TCP	In

OS	Rule	Definition	Port	Protocol	Direction
		allow RDP traffic.			
	Remote Desktop - User Mode (UDP-In)	Inbound rule for the Remote Desktop service to allow RDP traffic.	Local: 3389 Remote: Any	UDP	In

WindowsDevice Management

Windows Server 2022

OS	Rule	Definition	Port	Protocol	Direction
Windows Server 2022	WindowsDevice Management Certificate Installer (TCP out)	Allow outbound TCP traffic from WindowsDevice Management Certificate Installer.	Local: Any Remote: Any	TCP	Out
	WindowsDevice Management Device Enroller (TCP out)	Allow outbound TCP traffic from WindowsDevice Managemen	Local: Any Remote: 80, 443	TCP	Out

OS	Rule	Definition	Port	Protocol	Direction
		t Device Enroller.			
	WindowsDevice Management Enrollment Service (TCP out)	Allow outbound TCP traffic from WindowsDevice Management Enrollment Service.	Local: Any Remote: Any	TCP	Out
	WindowsDevice Management Sync Client (TCP out)	Allow outbound TCP traffic from WindowsDevice Management Sync Client.	Local: Any Remote: Any	TCP	Out

Windows Server 2019

OS	Rule	Definition	Port	Protocol	Direction
Windows Server 2019	WindowsDevice Management Certificate Installer (TCP out)	Allow outbound TCP traffic from WindowsDevice Managemen	Local: Any Remote: Any	TCP	Out

OS	Rule	Definition	Port	Protocol	Direction
		t Certificate Installer.			
	WindowsDevice Management Enrollment Service (TCP out)	Allow outbound TCP traffic from WindowsDevice Management Enrollment Service.	Local: Any Remote: Any	TCP	Out
	WindowsDevice Management Sync Client (TCP out)	Allow outbound TCP traffic from WindowsDevice Management Sync Client.	Local: Any Remote: Any	TCP	Out
	WindowsEnrollment WinRT (TCP Out)	Allow outbound TCP traffic from WindowsEnrollment WinRT.	Local: Any Remote: Any	TCP	Out

WindowsFeature Experience Pack

OS	Rule	Definition	Port	Protocol	Direction
Windows Server 2022	WindowsFeature Experience Pack	WindowsFeature Experience Pack.		Any	Out

WindowsFirewall Remote Management

OS	Rule	Definition	Port	Protocol	Direction
Windows Server 2012 R2	WindowsFirewall Remote Management (RPC)	Inbound rule for the WindowsFirewall to be remotely managed via RPC/TCP.	Local: RPC Remote: Any	TCP	In
	WindowsFirewall Remote Management (RPC-EPMAP)	Inbound rule for the RPCSS service to allow RPC/TCP traffic for the Windows Firewall.	Local: RPC-EPMap Remote: Any	TCP	In

WindowsRemote Management

OS	Rule	Definition	Port	Protocol	Direction
Windows Server 2012 Windows Server 2012 R2 Windows Server 2016 Windows Server 2019 Windows Server 2022	WindowsRemote Management (HTTP-In)	Inbound rule for WindowsRemote Management via WS-Management.	Local: 5985 Remote: Any	TCP	In

For more information about Amazon EC2 security groups, see Amazon EC2 Security Groups for WindowsInstances.

Updates applied for AWS Windows AMIs

To help ensure a smooth and consistent launch experience, AWS Windows AMIs include the following updates for initialization, installation, and configuration.

> **Note**
>
> When you launch an instance from an Amazon managed AWS Windows AMI, the root device for the Windows instance is an Amazon Elastic Block Store (Amazon EBS) volume. AWS Windows AMIs don't support instance store for the root device.

Clean and prepare

Description	Applies to
Check for pending file renames or reboots, and reboot as needed	All AMIs
Delete `.dmp` files	All AMIs
Delete logs (event logs, Systems Manager, EC2Config)	All AMIs
Delete temporary folders and files for Sysprep	All AMIs
Perform virus scan	All AMIs
Pre-compile queued .NET assemblies (before Sysprep)	All AMIs
Restore default values for Microsoft browsers	All AMIs
Reset the Windows wallpaper	All AMIs
Run Sysprep	All AMIs
Set EC2Launch v1 to run at the next launch	Windows Server 2016 and 2019
Run Windows maintenance tools	Windows Server 2012 R2 and later
Clear recent history (Start menu, Windows Explorer, and more)	Windows Server 2012 R2 and earlier
Restore default values for EC2Config	Windows Server 2012 R2 and earlier

Install and configure

Description	Applies to
Disable Secure Time Seeding	All AMIs

Description	Applies to
Add links to the Amazon EC2 Windows Guide	All AMIs
Attach instance storage volumes to extended mount points	All AMIs
Install the current AWS Tools for Windows PowerShell	All AMIs
Install the current CloudFormation bootstrap scripts	All AMIs
Disable RunOnce for Internet Explorer	All AMIs
Enable remote PowerShell	All AMIs
Disable hibernation and delete the hibernation file	All AMIs
Disable the Connected User Experiences and Telemetry service	All AMIs
Set the performance options for best performance	All AMIs
Set the power setting to high performance	All AMIs
Disable the screen saver password	All AMIs
Set the RealTimeIsUniversal registry key	All AMIs
Set the timezone to UTC	All AMIs
Disable Windows updates and notifications	All AMIs
Run Windows Update and reboot until there are no pending updates	All AMIs
Set the display in all power schemes to never turn off	All AMIs
Set the PowerShell execution policy to "Unrestricted"	All AMIs

Description	Applies to
If Microsoft SQL Server is installed: • Install service packs • Configure to start automatically • Add BUILTIN\Administrators to the SysAdmin role • Open TCP port 1433 and UDP port 1434	All AMIs
Configure a paging file on the system volume as follows: • Windows Server 2016 and later - Managed by the system • Windows Server 2012 R2 - Initial size and max size are 8 GB • Windows Server 2012 and earlier - Initial size is 512 MB, max size is 8 GB	All AMIs
Install the current EC2Launch v2 and SSM Agent	Windows Server 2022 and later
Install the current EC2Launch v1 and SSM Agent	Windows Server 2016 and 2019
Install the current SRIOV drivers	Windows Server 2012 R2 and later
Install the current EC2WinUtil driver	Windows Server 2008 R2 and later
Install the current EC2Config and SSM Agent	Windows Server 2012 R2 and earlier
Install the current AWS PV, ENA, and NVMe drivers	Windows Server 2008 R2 and later

Description	Applies to
Allow ICMP traffic through the firewall	Windows Server 2012 R2 and earlier
Configure an additional system managed paging file on `Z:`, if available	Windows Server 2012 R2 and earlier
Enable file and printer sharing	Windows Server 2012 R2 and earlier
Install the current Citrix PV driver	Windows Server 2008 SP2 and earlier
Install PowerShell 2.0 and 3.0	Windows Server 2008 SP2 and R2
Apply the following hotfixes: • MS15-011 • KB2582281 • KB2634328 • KB2394911 • KB2780879	Windows Server 2008 SP2 and R2

Changes in Windows Server AMIs by OS version

AWS provides AMIs for Windows Server 2016 and later. These AMIs include the following high-level changes between AWS Windows AMIs for different Windows operating system versions:

Windows Server 2025

- Windows Server 2025 AMIs use UEFI boot mode by default, except for Windows Server 2025 AMIs named `BIOS-Windows_Server-2025-English-Full-Base`.

> **Note**
>
> EC2 metal instance sizes and some EC2 instance types do not support UEFI boot mode for Windows Server. To launch Windows Server 2025 on these instances, you must use the AWS managed `BIOS-Windows_Server-2025-English-Full-Base` AMI, or an AMI that is based on that image. For more information about UEFI requirements, Requirements for UEFI boot mode in the *Amazon EC2 User Guide*.

- Windows Server 2025 AMIs support Nitro EC2 instance types only.
- Windows Server 2025 AMIs use gp3 EBS volume types by default.
- Windows Server 2025 AMIs use the AWS.Tools PowerShell module.

Windows Server 2016-2022

- To accommodate the change from .NET Framework to .NET Core, the EC2Config service has been deprecated on Windows Server 2016 AMIs and replaced by EC2Launch. EC2Launch is a bundle of Windows PowerShell scripts that perform many of the tasks performed by the EC2Config service. For more information, see Configure a Windows instance using EC2Launch. EC2Launch v2 replaces EC2Launch in Windows Server 2022 and later. For more information, see Configure a Windows instance using EC2Launch v2.
- On earlier versions of Windows Server AMIs, you can use the EC2Config service to join an EC2 instance to a domain and configure integration with Amazon CloudWatch. On Windows Server 2016 and later AMIs, you can use the CloudWatch agent to configure integration with Amazon CloudWatch. For more information about configuring instances to send log data to CloudWatch, see Collect Metrics and Logs from Amazon EC2 Instances and On-Premises Servers with the CloudWatch Agent. For information about joining an EC2 instance to a domain, see Join an Instance to a Domain Using the `AWS-JoinDirectoryServiceDomain` JSON Document in the *AWS Systems Manager User Guide*.

Other differences

Note the following additional important differences for instances created from Windows Server 2016 and later AMIs.

- By default, EC2Launch does not initialize secondary EBS volumes. You can configure EC2Launch to initialize disks automatically by either scheduling the script to run or by calling EC2Launch in

user data. For the procedure to initialize disks using EC2Launch, see "Initialize Drives and Drive Letter Mappings" in Configure EC2Launch.

- If you previously enabled CloudWatch integration on your instances by using a local configuration file (`AWS.EC2.Windows.CloudWatch.json`), you can configure the file to work with the SSM Agent on instances created from Windows Server 2016 and later AMIs.

AWS Windows AMI version history

The following tables summarize the changes to each release of the AWS Windows AMIs. Note that some changes apply to all AWS Windows AMIs, while others apply to only a subset of these AMIs.

For more information about components included in these AMIs, see the following:

- EC2Launch v2 version history
- EC2Launch v1 version history
- EC2Config version history
- Systems Manager SSM Agent Release Notes
- Amazon ENA driver versions
- AWS NVMe driver versions
- Paravirtual drivers for Windows instances
- AWS Tools for PowerShell Change Log

Monthly AMI updates for 2025 (to date)

For more information, see Description of Software Update Services and Windows Server Update Services changes in content for 2025 (KB894199) on the Microsoft website.

> **Note**
>
> Beginning January 2026, AWS Windows AMIs will ship with AWS.Tools for PowerShell version 5. This major version update includes changes that may impact existing scripts and workflows. For more information, review the following documents:
>
> - Migrating to V5 in the *AWS.Tools for PowerShell User Guide*
> - AWS.Tools for PowerShell V5 release announcement

Release	Changes
2025.12.10	**All AMIs** • AWS PowerShell version 4.1.953 • cfn-bookstrap version 2.0.37 • SSM Agent version 3.3.3185.0 • Windows Security Updates current to December 9, 2025 Previous versions of Amazon-published AWS Windows AMIs dated September 10, 2025 and earlier will be made private after January 12, 2026, 10 AM Pacific.
2025.11.20	**New AWS Windows AMIs with Microsoft SQL Server 2025.** • Windows_Server-2025-English-Full-SQL_2025_Enterprise • Windows_Server-2025-English-Full-SQL_2025_Standard • Windows_Server-2025-English-Full-SQL_2025_Express • Windows_Server-2025-Japanese-Full-SQL_2025_Enterprise • Windows_Server-2025-Japanese-Full-SQL_2025_Standard • Windows_Server-2025-Korean-Full-SQL_2025_Enterprise • Windows_Server-2025-Korean-Full-SQL_2025_Standard
2025.11.12	**All AMIs** • AWS PowerShell version 4.1.935 •

Release	Changes

	EC2Launch v2 version 2.3.56
	• SQL Server GDR installed:
	  • SQL_2022: KB5068406
	  • SQL_2019: KB5068404
	  • SQL_2017: KB5068402
	  • SQL_2016: KB5068401
	• Windows Security Updates current to November 11, 2025
	
	Previous versions of Amazon-published AWS Windows AMIs dated August 13, 2025 and earlier will be made private after December 8, 2025, 10 AM Pacific.

2025.10.15	**All AMIs** • AWS PowerShell version 4.1.915 • AWS NVMe driver version 1.7.0 • EC2Launch v1 version 1.4.6 • Windows Security Updates current to October 15, 2025 Previous versions of Amazon-published AWS Windows AMIs dated July 9, 2025 and earlier will be made private after November 10, 2025, 10 AM Pacific.

Release	Changes

2025.09.10	**All AMIs**
	• AWS PowerShell version 4.1.892
	• cfn-bootstrap v2.0.36
	• Elastic Network Adapter (ENA) version 2.11.0
	• SSM Agent version 3.3.3050.0
	• SQL Server GDR installed:
	  • SQL_2022: KB5065220
	  • SQL_2019: KB5065222
	  • SQL_2017: KB5065225
	  • SQL_2016: KB5065226
	• Windows Security Updates current to September 9, 2025
	
	Previous versions of Amazon-published AWS Windows AMIs dated June 11, 2025 and earlier will be made private after October 13, 2025, 10 AM Pacific.

Release	Changes

2025.08.13	**All AMIs**
	• AWS PowerShell version 4.1.872
	• EC2Launch v2 version 2.2.63
	• Elastic Network Adapter (ENA) version 2.10.0
	• SSM Agent version 3.3.2656.0
	• SQL Server GDR installed:
	  • SQL_2022: KB5063814
	  • SQL_2019: KB5063757
	  • SQL_2017: KB5063759
	  • SQL_2016: KB5063762
	• Windows Security Updates current to August 12, 2025
	
	Previous versions of Amazon-published AWS Windows AMIs dated May 15, 2025 and earlier will be made private after September 8, 2025, 10 AM Pacific.
	New Windows AMIs:
	• `Windows_Server-2025-French-Full-Base`
	• `Windows_Server-2025-German-Full-Base`

Release	Changes

2025.07.09	**All AMIs**
	• AWS PowerShell version 4.1.853
	• SSM Agent version 3.3.2471.0
	• SQL Server GDR installed:
	  • SQL_2022: KB5058721
	  • SQL_2019: KB5058722
	  • SQL_2017: KB5058714
	  • SQL_2016: KB5058718
	• Windows Security Updates current to July 8, 2025
	
	Previous versions of Amazon-published AWS Windows AMIs dated April 9, 2025 and earlier will be made private after August 11, 2025, 10 AM Pacific.
	
	Note
	The following image types are no longer receiving updates and the final versions will become private after September 8th, 2025. If you wish to retain access to one of these image types, you can create a copy in your account prior to this date.
	• Windows_Server-2016-English-Core-SQL_2016_SP3_Enterprise
	• Windows_Server-2016-English-Core-SQL_2016_SP3_Standard
	• Windows_Server-2016-English-Core-SQL_2016_SP3_Web
	•

Release	Changes
	Windows_Server-2016-English-Full-HyperV • Windows_Server-2016-English-Tesla • Windows_Server-2016-Japanese-Full-SQL_2016_SP3_Enterprise • Windows_Server-2016-Japanese-Full-SQL_2016_SP3_Express • Windows_Server-2016-Japanese-Full-SQL_2016_SP3_Standard • Windows_Server-2016-Japanese-Full-SQL_2016_SP3_Web • Windows_Server-2019-English-Full-HyperV
2025.06.11	**All AMIs** • AWS PowerShell version 4.1.834 • AWS PV driver version 8.6.0 • EC2Launch v2 version 2.1.1 • SQL Server CUs installed: • SQL_2022: CU 19 • Windows Security Updates current to June 10, 2025 Previous versions of Amazon-published AWS Windows AMIs dated March 12, 2025 and earlier will be made private after July 7, 2025, 10 AM Pacific.

Release	Changes
2025.05.15	**All AMIs** • AWS PowerShell version 4.1.814 • SSM Agent version 3.3.2299.0 • Windows Security Updates current to May 13, 2025 New Windows AMIs: `BIOS-Windows_Server-2025-English-Core-Base`. Previous versions of Amazon-published AWS Windows AMIs dated Febuary 12, 2025 and earlier will be made private after June 9, 2025, 10 AM Pacific.
2025.04.09	**All AMIs** • AWS PowerShell version 4.1.791 • cfn-bootstrap v2.0.34 • EC2Launch v2 version 2.0.2107 • SSM Agent version 3.3.1957.0 • SQL Server CUs installed: • SQL_2022: CU 18 • Windows Security Updates current to April 8, 2025 Previous versions of Amazon-published AWS Windows AMIs dated January 15, 2025 and earlier will be made private after May 13, 2025, 10 AM Pacific.

Release	Changes
2025.03.12	**All AMIs** • AWS PowerShell version 4.1.771 • cfn-bootstrap v2.0.33 • EC2Launch v1 version 1.3.2005119 • EC2Launch v2 version 2.0.2081 • SQL Server CUs installed: • SQL_2019: CU 32 • Windows Security Updates current to March 11, 2025 Previous versions of Amazon-published AWS Windows AMIs dated December 13, 2024 and earlier will be made private after April 8, 2025, 10 AM Pacific. **Note** Beginning March 2025, R Services and Machine Learning Services with R and Python runtimes are no longer enabled by default on SQL Server 2016, 2017, and 2019 AMIs. These features include runtimes that are not maintained through SQL server cumulative updates. You can enable these features on your instance launched from our SQL Server AMIs using the SQL installation media included at C:\SQLServerSetup.

Release	Changes
2025.02.13	**All AMIs** • AWS PowerShell version 4.1.749 • SSM Agent version 3.3.1611.0 • SQL Server CUs installed: • SQL_2022: CU 17 • Windows Security Updates current to February 12, 2025 Previous versions of Amazon-published AWS Windows AMIs dated November 19, 2024 and earlier will be made private after March 11, 2025, 10 AM Pacific.
2025.01.15	**All AMIs** • AWS PowerShell version 4.1.731 • cfn-init v2.0.32 • Elastic Network Adapter (ENA) version 2.9.0 • Windows Security Updates current to January 14, 2025 Previous versions of Amazon-published AWS Windows AMIs dated October 9, 2024 and earlier will be made private after February 11, 2025, 10 AM Pacific.

Monthly AMI updates for 2024

For more information, see Description of Software Update Services and Windows Server Update Services changes in content for 2024 on the Microsoft website.

Release	Changes
2024.12.13	**All AMIs** • AWS PowerShell version 4.1.713 • AWS PV driver version 8.5.0 • SQL Server CUs installed: • SQL_2019: CU 30 • Windows Security Updates current to December 10, 2024 Previous versions of Amazon-published AWS Windows AMIs dated September 11, 2024 and earlier will be made private after January 15, 2025, 10 AM Pacific.
2024.11.19	**All AMIs** • SSM Agent version 3.3.1345.0 This SSM Agent version addresses an issue where Windows Server 2025 instances may not connect to Systems Manager Sessions Manager or Fleet Manager RDP.

Release	Changes
	Note This is a partial release. Only Windows Server 2025 AMIs are included in this release.

2024.11.13	**All AMIs**
	• AWS PowerShell version 4.1.694
	• AWS NVMe driver version 1.6.0
	• cfn-init v2.0.31
	• EC2Launch v1 version 1.3.2005065
	• SSM Agent version 3.3.1230.0
	• SQL Server CUs installed:
	  • SQL_2022: GDR KB5046862
	  • SQL_2019: CU 29 + GDR KB5046860
	  • SQL_2017: GDR KB5046858
	  • SQL_2006_SP3: KB5046855
	• Windows Security Updates current to Nobember 12, 2024
	
	Previous versions of Amazon-published AWS Windows AMIs dated August 14, 2024 and earlier will be made private after December 11, 2024, 10 AM Pacific.

Release	Changes
2024.11.04	Release AMIs for Windows Server 2025. Windows Server 2025 AMIs are configured with UEFI boot-mode, gp3 root volumes, and have IMDS V2 enabled by default. A BIOS configured AMI is available for use on Bare Metal platforms and Nitro instances where UEFI support is not available. • AWS.Tools version 4.1.691 AWS.Tools PowerShell modules is a modularized version of the PowerShell toolset that reduces module load time. For more informati on see the AWS Tools for PowerShell User Guide. • SSM Agent version 3.3.1230.0 • You may encounter an issue connecting AWS Systems Manager Sessions Manager to a Windows Server 2025 instance. To address this issue, log onto the instance, then navigate to `Settings > Apps > Optional Features` , and add `WMIC`. Restart the SSM Agent service or reboot the instance, and Sessions Manager should connect. • Windows Credential Guard is not supported on EC2 instances running Windows Server 2025.

Release	Changes

2024.10.09	**All AMIs**
	• AWS Tools for Windows PowerShell version 4.1.667
	• EC2Launch v2 version 2.0.2046
	• Elastic Network Adapter (ENA) version 2.8.0
	• SSM Agent version 3.3.859.0
	• SQL Server CUs installed:
	  • SQL_2022: CU15 + GDR KB5046059
	  • SQL_2019: GDR KB5046060
	  • SQL_2017: GDR KB5046061
	  • SQL_2016_SP3: GDR KB5046063
	• Windows Security Updates current to October 8, 2024
	
	Previous versions of Amazon-published AWS Windows AMIs dated July 10, 2024 and earlier will be made private after November 11, 2024, 10 AM Pacific.
	
	Note
	Starting in October, default root volume sizes on some AMIs changed to provide additional free space for the configuration changes applied to the images. For all Core or Full Base Images, including EC2Launch v2 and TPM versions, the root volume size remains 30GB. For all Windows AMIs with SQL Server, the root

Release	Changes
	volume size is now 75GB. For all other Windows AMI configurations, the root volume size is now 50GB.

2024.09.11	**All AMIs**
	• AWS Tools for Windows PowerShell version 4.1.648
	• SQL Server CUs installed:
	  • SQL_2022: GDR KB5042578
	  • SQL_2019: GDR KB5042749
	  • SQL_2017: GDR KB5042215
	  • SQL_2016_SP3: GDR KB5042207
	• Windows Security Updates current to September 10, 2024
	
	Previous versions of Amazon-published AWS Windows AMIs dated June 13, 2024 and earlier will be made private after October 7, 2024, 10 AM Pacific.

Release	Changes

2024.08.14	**All AMIs**
	• AWS Tools for Windows PowerShell version 4.1.628
	• EC2Launch v1 version 3.2005008
	• EC2Launch v2 version 2.0.1981
	• SQL Server CUs installed:
	  • SQL_2022: CU 14
	  • SQL_2019: CU 28
	  • SQL_2017: GDR KB5040940
	  • SQL_2016_SP3: GDR KB5040946
	• Windows Security Updates current to August 13, 2024
	
	Previous versions of Amazon-published AWS Windows AMIs dated May 15, 2024 and earlier will be made private after September 9, 2024, 10 AM Pacific.

Release	Changes
2024.07.10	**All AMIs** • AWS Tools for Windows PowerShell version 4.1.611 • EC2Launch v1 version 3.2004959 • EC2Launch v2 version 2.0.1948 • SSM Agent version 3.3.551.0 • SQL Server CUs installed: • SQL_2019: CU 27 • NVIDIA Tesla version 475.14 • Windows Security Updates current to July 10, 2024 Previous versions of Amazon-published AWS Windows AMIs dated April 10, 2024 and earlier will be made private after August 12, 2024, 10 AM Pacific.

Release	Changes
2024.06.13	**All AMIs** • AWS Tools for Windows PowerShell version 4.1.593 • EC2Launch v1 version 3.2004891 • EC2Launch v2 version 2.0.1924 • EC2WinUtil version 3.0.0 • Elastic Network Adapter (ENA) version 2.7.0 • SSM Agent version 3.3.484.0 • SQL Server CUs installed: • SQL_2022: CU 13 • NVIDIA Tesla version 475.06 • Windows Security Updates current to June 11, 2024 Previous versions of Amazon-published AWS Windows AMIs dated March 13, 2024 and earlier will be made private after July 8, 2024, 10 AM Pacific.

Release	Changes

2024.05.15	**All AMIs**
	• AWS Tools for Windows PowerShell version 4.1.575
	• EC2Launch v2 version 2.0.1881
	• SSM Agent version 3.3.380.0
	• SQL Server CUs installed:
	  • SQL_2022: GDR KB5036343
	  • SQL_2019: CU26
	• Windows Security Updates current to May 14, 2024
	
	Previous versions of Amazon-published AWS Windows AMIs dated February 14, 2024 and earlier will be made private after June 10, 2024, 10 AM Pacific.

Release	Changes
2024.04.10	**All AMIs** • Windows Security Updates current to April 9, 2024 • AWS Tools for Windows PowerShell version 4.1.551 • SSM Agent version 3.3.131.0 • SQL Server CUs installed: • SQL_2022: CU12 Previous versions of Amazon-published AWS Windows AMIs dated January 16, 2024 and earlier will be made private after May 13, 2024, 10 AM Pacific.

Release	Changes
2024.03.13	**All AMIs** • Windows Security Updates current to March 12, 2024 • AWS Tools for Windows PowerShell version 4.1.530 • EC2Launch v2 version 2.0.1815 • SSM Agent version 3.2.2303.0 • NVIDIA GRID Driver version 538.33 • NVIDIA Tesla Driver version 474.82 • SQL Server CUs installed: • SQL_2019: CU25 **Note** To ensure that you always receive valid time from your configure d Network Time Protocol (NTP) service, Secure Time Seeding (STS) is disabled on all AWS Windows AMIs from this version forward. Amazon Time Sync Service is the default NTP service for all AWS Windows AMIs that Amazon provides. Previous versions of Amazon-published AWS Windows AMIs dated December 13, 2023 and earlier will be made private after April 8, 2024, 10 AM Pacific.

Release	Changes
2024.02.14	**All AMIs** • Windows Security Updates current to Febuary 13, 2024 • AWS Tools for Windows PowerShell version 4.1.512 • cfn-init version 2.0.29 • SSM Agent version 3.2.2222.0 • SQL Server CUs installed: • SQL_2022: CU11 Previous versions of Amazon-published AWS Windows AMIs dated November 15, 2023 and earlier will be made private after March 11, 2024, 10 AM Pacific.
2024.01.16	**All AMIs** • EC2Launch v2 version 2.0.1739 • EC2Launch v1 v1 version 1.3.2004617

Release	Changes
2024.01.10 (*Deprecated*)	**Note** *Due to functional issues with EC2Launch v1 and EC2Launch v2, this AMI version is marked as deprecated. The AMIs are still available for launch, and are described by directly referencing their AMI ID. However, they will no longer appear in search results for public AMIs. We recommend that you use the latest AMI version, dated 2024.01.16.* **All AMIs** • Windows Security Updates current to January 9, 2024 *Note:* Due to a known update installation issue, we excluded the standalone Windows update KB5034439 on Windows Server 2022 Core AMIs. The update only applies to Windows installations with a separate WinRE partition. These partitions are not included with our EC2 Windows Server AMIs. For more information, see KB5042322: Windows Recovery Environment update for Windows Server 2022: January 9, 2024 on the Microsoft website. • AWS Tools for PowerShell version 4.1.486 • EC2Launch v1 v1 version 1.3.2004592 • EC2Launch v2 version 2.0.1702 • SQL Server CUs installed: • SQL_2019: CU24

Release	Changes
	Previous versions of Amazon-published AWS Windows AMIs dated October 11, 2023 and earlier will be made private after February 12th 2024, 10 AM Pacific.

Monthly AMI updates for 2023

For more information, see Description of Software Update Services and Windows Server Update Services changes in content for 2023 on the Microsoft website.

Release	Changes
2023.12.13	**All AMIs** • Windows Security Updates current to December 12, 2023 • AWS Tools for PowerShell version 4.1.468 • AMD Radeon Pro Driver version 22.10.01.12 • NVIDIA GRID Driver version 537.70 • NVIDIA Tesla Driver version 474.64 • SQL Server CUs installed: • SQL_2022: CU10 Previous versions of Amazon-published AWS Windows AMIs dated Sep tember 13, 2023 and earlier will be made private after January 8th 2024, 10 AM Pacific.
2023.11.15	

Release	Changes

	All AMIs
	• Windows Security Updates current to November 14, 2023
	• AWS Tools for PowerShell version 4.1.447
	• EC2Launch v1 version 1.3.2004491
	• SSM Agent version 3.2.1705.0
	• SQL Server CUs installed:
	  • SQL_2022: CU9
	  • SQL_20219: CU23
	• SQL Server GDRs installed:
	  • SQL 2017: KB5029376
	  • SQL 2016: KB5029186
	  • SQL 2014: KB5029185
	
	Previous versions of Amazon-published AWS Windows AMIs dated August 10, 2023 and earlier were made private.

Release	Changes
2023.10.11	**All AMIs** • Windows Security Updates current to October 10, 2023 • cfn-init version 2.0.28 • EC2Launch v1 version 1.3.2004438 • EC2Launch v2 version 2.0.1643 • SSM version 3.2.1630.0 • AWS Tools for PowerShell version 4.1.426 • SQL Server CUs installed: • SQL_2022: CU8 Previous versions of Amazon-published AWS Windows AMIs dated July 12, 2023 and earlier were made private.

Release	Changes

2023.09.13	**All AMIs**
	• Windows Security Updates current to September 12, 2023
	• EC2Launch v2 version 2.0.1580
	• SSM version 3.2.1377.0
	• AWS Tools for PowerShell version 4.1.407
	• AWS NVMe driver version 1.5.0
	• SQL Server CUs installed:
	  • SQL_2022: CU7
	  • SQL_2019: CU22
	
	Windows Server 2012 RTM and Window Server 2012 R2 will reach End of Support (EOS) on October 10, 2023 and will no longer receive regular security updates from Microsoft. On this date, AWS will no longer publish or distribute Windows Server 2012 RTM or Windows Server 2012 R2 AMIs. Existing instances running Windows Server 2012 RTM and Windows Server 2012 R2 will not be impacted. Custom AMIs in your account will also not be impacted. You can continue to use them normally after the EOS date.
	
	Previous versions of Amazon-published AWS Windows AMIs dated June 14, 2023 and earlier were made private.

Release	Changes
2023.08.10	**All AMIs** • Windows Security Updates current to August 8, 2023 • AWS Tools for PowerShell version 4.1.383 • EC2Config version 4.9.5467 • SSM version 3.1.2282.0 • AWS ENA version 2.6.0 • cfn-init version 2.0.26 • SQL Server CUs installed: • SQL_2022: CU6 Windows Server 2012 RTM and Window Server 2012 R2 will reach End of Support (EOS) on October 10, 2023 and will no longer receive regular security updates from Microsoft. On this date, AWS will no longer publish or distribute Windows Server 2012 RTM or Windows Server 2012 R2 AMIs. Existing instances running Windows Server 2012 RTM and Windows Server 2012 R2 will not be impacted. Custom AMIs in your account will also not be impacted. You can continue to use them normally after the EOS date. Previous versions of Amazon-published AWS Windows AMIs dated May 10, 2023 and earlier were made private.

Release	Changes

2023.07.12	**All AMIs**
	• Windows Security Updates current to July 11, 2023
	• AWS Tools for Windows PowerShell version 4.1.366
	• EC2Launch v1 version 1.3.2004256
	• EC2Launch v2 version 2.0.1521
	• SQL Server CUs installed:
	  • SQL_2022: CU5
	  • SQL_2019: CU21
	
	.NET Framework 3.5 is now enabled in Windows Server 2012 R2 AMIs due to Microsoft security updates. If these updates are applied before .NET 3.5 is enabled, it is no longer possible to enable the feature. If you prefer to disable .NET 3.5, you can do so through Server Manager or `dism` commands.
	
	Previous versions of Amazon-published AWS Windows AMIs dated April 12, 2023 and earlier were made private.

Release	Changes
2023.06.14	**All AMIs** • Windows Security Updates current to June 13, 2023 • AWS Tools for Windows PowerShell version 4.1.346 • SQL Server CUs installed: • SQL_2022: CU4 The AWS Tools for Windows installation package has been deprecated, and no longer appears as an installed program in AWS Windows AMIs provided by AWS. The AWSPowerShell Module is now installed at `C:\ProgramFiles\WindowsPowerShell\Modules\AWSPowerShell`. The .NET SDK remains located at `C:\ProgramFiles (x86)\AWS SDK for .NET`. For more information see the blog announcement. Windows Server 2012 RTM and Windows Server 2012 R2 will reach End of Support (EOS) on October 10, 2023 and will no longer receive regular security updates from Microsoft. On this date, AWS will no longer publish or distribute Windows Server 2012 RTM or Windows Server 2012 R2 AMIs. Existing RTM/R2 instances and custom AMIs in your account will not be impacted, and you can continue to use them after the EOS date. For more information about Microsoft End of Support on AWS, including upgrade and import options, as well as a full list of AMIs that will no longer be published or distributed on October 10, 2023, see the End of Support for Microsoft Products FAQ. Previous versions of Amazon-published AWS Windows AMIs dated March 15, 2023 and earlier were made private.

Release	Changes

2023.05.10	**All AMIs**
	• Windows Security Updates current to May 9, 2023
	• AWS Tools for Windows PowerShell version 3.15.2072
	• EC2Launch v2 version 2.0.1303
	• cfn-init version 2.0.25
	• SQL Server CUs installed:
	  • SQL_2022: CU3
	  • SQL_2019: CU20
	
	Previous versions of Amazon-published AWS Windows AMIs dated February 15, 2023 and earlier were made private.

Release	Changes
2023.04.12	**All AMIs** • Windows Security Updates current to April 11, 2023 • AWS Tools for Windows PowerShell version 3.15.2035 • AWS NVMe driver version 1.4.2 • SQL Server CUs installed: • SQL_2022: CU 2 • SSM version 3.1.2144.0 **Windows Server 2016, 2019, and 2022** • Intel 82599 VF driver version 2.1.249.0 **Windows Server 2012 R2** • Intel 82599 VF driver version 1.2.317.0 Previous versions of Amazon-published AWS Windows AMIs dated January 19, 2023 and earlier were made private.

Release	Changes

2023.03.15	**All AMIs**
	• Windows Security Updates current to March 14, 2023
	• AWS Tools for Windows PowerShell version 3.15.1998
	• EC2Config version 4.9.5288
	• EC2Launch v1 version 1.3.2004052
	• EC2Launch v2 version 2.0.1245
	• cfn-init version 2.0.24
	• SQL Server CUs installed:
	  • SQL_2022: CU 1
	  • SQL_2019: CU 19
	• SQL Server GDRs installed:
	  • SQL_2017: KB5021126
	  • SQL_2016: KB5021129
	  • SQL_2014: KB5021045
	
	Previous versions of Amazon-published AWS Windows AMIs dated December 28, 2022 and earlier were made private.

Release	Changes
2023.02.15	**All AMIs** • Windows Security Updates current to February 14, 2023 • AWS Tools for Windows PowerShell version 3.15.1958 • AWS PV version 8.4.3 **New AWS Windows AMIs** • TPM-Windows_Server-2019-English-Full-SQL_2019_Enterprise • TPM-Windows_Server-2019-English-Full-SQL_2019_Standard • TPM-Windows_Server-2022-English-Full-SQL_2022_Enterprise • TPM-Windows_Server-2022-English-Full-SQL_2022_Standard New AWS Windows AMIs with Microsoft SQL Server with support for NitroTPM and UEFI Secure Boot have been released. The images include Windows Server 2019 or Windows Server 2022 with SQL Server 2019 or SQL Server 2022. Each SQL Server version is available in Standard and Enterprise editions. Previous versions of Amazon-published AWS Windows AMIs dated November 21, 2022 and earlier were made private.

Release	Changes
2023.01.19	**All AMIs** • cfn-init version 2.0.21 Previous versions of Amazon-published AWS Windows AMIs dated October 27, 2022 and earlier were made private.
2023.01.11	**All AMIs** • Windows Security updates current to January 10, 2023 • AWS Tools for Windows PowerShell version 3.15.1919 • EC2Launch v1 version 1.3.2003975 • EC2Launch v2 version 2.0.1121

Monthly AMI updates for 2022

For more information, see Description of Software Update Services and Windows Server Update Services changes in content for 2022 on the Microsoft website.

Release	Changes
2022.12.28	**Windows Server 2016 and 2019 AMIs** • EC2Launch v1 version 1.3.2003975
2022.12.14	**All AMIs** • Windows Security updates current to December 13th, 2022

Release	Changes
	• AWS Tools for Windows PowerShell version 3.15.1886 • EC2Config version 4.9.5103 • EC2Launch v1 version 1.3.2003961 • EC2Launch v2 version 2.0.1082 • SSM version 3.1.1856.0 • cfn-init version 2.0.19

Release	Changes
2022.11.21	**New AWS Windows AMIs** • Windows_Server-2019-English-Full-SQL_2022_Enterprise • Windows_Server-2019-English-Full-SQL_2022_Express • Windows_Server-2019-English-Full-SQL_2022_Standard • Windows_Server-2019-English-Full-SQL_2022_Web • Windows_Server-2019-Japanese-Full-SQL_2022_Enterprise • Windows_Server-2019-Japanese-Full-SQL_2022_Standard • Windows_Server-2019-Japanese-Full-SQL_2022_Web • Windows_Server-2022-English-Full-SQL_2022_Enterprise • Windows_Server-2022-English-Full-SQL_2022_Express • Windows_Server-2022-English-Full-SQL_2022_Standard • Windows_Server-2022-English-Full-SQL_2022_Web • Windows_Server-2022-Japanese-Full-SQL_2022_Enterprise • Windows_Server-2022-Japanese-Full-SQL_2022_Standard • Windows_Server-2022-Japanese-Full-SQL_2022_Web Previous versions of Amazon-published AWS Windows AMIs dated August 10, 2022 and earlier were made private.

Release	Changes
2022.11.17	**All AMIs** • EC2Config version 4.9.5064. This is an out of band release for images that use EC2Config as the default launch agent. This includes all Windows Server 2012 RTM and Windows Server 2012 R2 AMIs. This release updates EC2Config to the latest version to improve support for our newest EC2 instance types.

2022.11.10	**All AMIs**
	
	• Windows Security updates current to November 8th, 2022
	• AWS Tools for Windows PowerShell version 3.15.1846
	• EC2Launch v1 version 1.3.2003923
	• EC2Launch v2 version 2.0.1011
	• SQL Server CUs installed:
	  • SQL_2019: CU 18
	  • SQL_2017: CU 31
	• cfn-init version 2.0.18

Release	Changes
2022.10.27	**All AMIs** • Out-of-band updates applied to resolve issues resulting from October patches. For more information, see Windows release health on the Microsoft website. Previous versions of Amazon-published AWS Windows AMIs dated July 13, 2022 and earlier were made private.
2022.10.12	**All AMIs** • Windows Security updates current to October 11th, 2022 • AWS Tools for Windows PowerShell version 3.15.1809 • EC2Launch v1 version 1.3.2003857 • SSM version 3.1.1732.0 • cfn-init version 2.0.16

Release	Changes
2022.09.14	**All AMIs** • Windows Security updates current to September 13th, 2022 • AWS Tools for Windows PowerShell version 3.15.1772 • EC2Launch v1 version 1.3.2003824 • SQL Server CU installed: • SQL_2019: CU17 Previous versions of Amazon-published AWS Windows AMIs dated June 15, 2022 and earlier were made private.
2022.08.10	**All AMIs** • Windows Security updates current to August 9th, 2022 • AWS Tools for Windows PowerShell version 3.15.1737 • cfn-init version 2.0.15 • SSM version 3.1.1634.0 (only AMIs that include EC2Launch v1 v1 or v2) • SQL Server CU installed: • SQL_2017: CU30 Previous versions of Amazon-published AWS Windows AMIs dated May 25, 2022 and earlier were made private.

Release	Changes

2022.07.13	**All AMIs**
	
	• Windows Security updates current to July 12th, 2022
	• AWS Tools for Windows PowerShell version 3.15.1706
	• cfn-init version 2.0.12
	• EC2Launch v1 version 1.3.2003691
	• EC2Launch v2 version 2.0.863
	• SQL Server GDRs installed:
	  • SQL_2019: KB5014353
	  • SQL_2017: KB5014553
	  • SQL_2016: KB5014355
	  • SQL_2014: KB5014164
	
	Windows Server version 20H2 will reach end-of-support on August 9, 2022. Existing instances and custom images owned by your account that are based on Windows Server version 20H2 will not be impacted. If you would like to retain access to Windows Server version 20H2, create a custom image in your account prior to August 9, 2022. All public versions of the following images will be made private on the end-of-support date.
	
	• Windows_Server-20H2-English-Core-Base
	• Windows_Server-20H2-English-Core-ContainersLatest

Release	Changes
	Previous versions of Amazon-published AWS Windows AMIs dated April 13, 2022 and earlier were made private.

Release	Changes
2022.06.15	**All AMIs** • Windows Security updates current to June 14th, 2022 • AWS Tools for Windows PowerShell version 3.15.1678 • AWS NVMe version 1.4.1 • EC2Config version 4.9.4588 • EC2Launch v1 version 1.3.2003639 • SSM version 3.1.1188.0 Microsoft SQL Server 2012 is reaching end-of-support on July 12th, 2022. All public versions of the following images have been made private. Existing instances and custom images owned by your account that are based on Windows Server images containing SQL Server 2012 will not be impacted. • Windows_Server-2012-R2_RTM-English-64Bit-SQL_2012_SP4_Enterprise-* • Windows_Server-2012-RTM-English-64Bit-SQL_2012_SP4_Enterprise-* • Windows_Server-2012-RTM-English-64Bit-SQL_2012_SP4_Express-* • Windows_Server-2012-RTM-English-64Bit-SQL_2012_SP4_Standard-* • Windows_Server-2012-RTM-English-64Bit-SQL_2012_SP4_Web-* • Windows_Server-2012-RTM-Japanese-64Bit-SQL_2012_SP4_Express-* • Windows_Server-2012-RTM-Japanese-64Bit-SQL_2012_SP4_Standard-* • Windows_Server-2012-RTM-Japanese-64Bit-SQL_2012_SP4_Web-*

Release	Changes
	• Windows_Server-2016-English-64Bit-SQL_2012_SP4_Enterprise-* • Windows_Server-2016-English-Full-SQL_2012_SP4_Standard-* For more information on Windows Server product lifecycles, please consult the following Microsoft documentation and AWS Microsoft FAQ: • Microsoft SQL Server 2012 • End-of-Support for Microsoft Products
2022.05.25	**All AMIs** • Out-of-band updates applied to resolve issues resulting from May patches. For more information, see Windows release health on the Microsoft website. Previous versions of Amazon-published AWS Windows AMIs dated February 10, 2022 and earlier were made private.

Release	Changes

2022.05.11	**All AMIs**
	• Windows Security updates current to May 10th, 2022
	• AWS Tools for Windows PowerShell version 3.15.1643
	• AWS PV version 8.4.2
	• AWS ENA version 2.4.0
	• SQL Server CUs installed:
	  • SQL_2019: CU 16
	  • SQL_2017: CU 29

2022.05.05	**New AWS Windows AMIs** New AWS Windows AMIs with support for NitroTPM and UEFI Secure Boot have been released. These images feature EC2Launch v2 as the default launch agent. They are available to launch on any instance type that supports NitroTPM and UEFI boot mode. • TPM-Windows_Server-2022-English-Core-Base-2022.05.05 • TPM-Windows_Server-2022-English-Full-Base-2022.05.05 • TPM-Windows_Server-2019-English-Core-Base-2022.05.05 • TPM-Windows_Server-2019-English-Full-Base-2022.05.05 • TPM-Windows_Server-2016-English-Core-Base-2022.05.05 • TPM-Windows_Server-2016-English-Full-Base-2022.05.05

Release	Changes
2022.04.13	**All AMIs** • Windows Security updates current to April 12th, 2022 • AWS Tools for Windows PowerShell version 3.15.1620 Previous versions of Amazon-published AWS Windows AMIs dated January 21, 2022 and earlier were made private. After June 2022, we will no longer release updated versions of the following images that include SQL Server 2016 SP2. SQL Server SP3 AMIs are available and will continue to be updated and released monthly. • Windows_Server-2019-English-Full-SQL_2016_SP2_Web • Windows_Server-2019-English-Full-SQL_2016_SP2_Standard • Windows_Server-2019-English-Full-SQL_2016_SP2_Express • Windows_Server-2019-English-Full-SQL_2016_SP2_Enterprise • Windows_Server-2016-Korean-Full-SQL_2016_SP2_Standard • Windows_Server-2016-Japanese-Full-SQL_2016_SP2_Web • Windows_Server-2016-Japanese-Full-SQL_2016_SP2_Standard • Windows_Server-2016-Japanese-Full-SQL_2016_SP2_Express • Windows_Server-2016-Japanese-Full-SQL_2016_SP2_Enterprise • Windows_Server-2016-English-Full-SQL_2016_SP2_Web • Windows_Server-2016-English-Full-SQL_2016_SP2_Standard •

Release	Changes
	Windows_Server-2016-English-Full-SQL_2016_SP2_Express • Windows_Server-2016-English-Full-SQL_2016_SP2_Enterprise • Windows_Server-2016-English-Core-SQL_2016_SP2_Web • Windows_Server-2016-English-Core-SQL_2016_SP2_Standard • Windows_Server-2016-English-Core-SQL_2016_SP2_Express • Windows_Server-2016-English-Core-SQL_2016_SP2_Enterprise • Windows_Server-2012-R2_RTM-Japanese-64Bit-SQL_2016_SP2_Web • Windows_Server-2012-R2_RTM-Japanese-64Bit-SQL_2016_SP2 _Standard • Windows_Server-2012-R2_RTM-Japanese-64Bit-SQL_2016_SP2_Express • Windows_Server-2012-R2_RTM-Japanese-64Bit-SQL_2016_SP2_Enterpri se • Windows_Server-2012-R2_RTM-English-64Bit-SQL_2016_SP2_Web • Windows_Server-2012-R2_RTM-English-64Bit-SQL_2016_SP2_Standard • Windows_Server-2012-R2_RTM-English-64Bit-SQL_2016_SP2_Express • Windows_Server-2012-R2_RTM-English-64Bit-SQL_2016_SP2_Enterprise

Release	Changes
2022.03.09	**All AMIs** • Windows Security updates current to March 8th, 2022 • AWS Tools for Windows PowerShell version 3.15.1583 • AWS ENA version 2.2.3 (reverted due to potential performance degradation on 6th generation EC2 instances) • EC2Config version 4.9.4556 • SSM version 3.1.1045.0 • SQL Server CUs installed: • SQL_2019: CU 15 Previous versions of Amazon-published AWS Windows AMIs dated December 12, 2021 and earlier were made private.

Release	Changes
2022.02.10	**All AMIs** • Windows Security updates current to February 8th, 2022 • AWS Tools for Windows PowerShell version 3.15.1546 • cfn-init version 2.0.10 • EC2Config version 4.9.4536 • EC2Launch v1 version 1.3.2003498 • EC2Launch v2 version 2.0.698 • SSM version 3.1.804.0 • SQL Server CUs installed: • SQL_2017: CU 28 Previous versions of Amazon-published AWS Windows AMIs dated Nove mber 16, 2021 and earlier were made private.
2022.01.19	**All AMIs** • Out-of-band updates applied to resolve issues resulting from January patches. For more information, see Windows release health on the Microsoft website. Previous versions of Amazon-published AWS Windows AMIs dated October 13, 2021 and earlier were made private.

Release	Changes
2022.01.12	**All AMIs** • Windows Security updates current to January 11th, 2022 • AWS Tools for Windows PowerShell version 3.15.1511 • AWS PV version 8.4.1 • SQL Server CUs installed: • SQL_2019: CU 14

Monthly AMI updates for 2021

For more information, see Description of Software Update Services and Windows Server Update Services changes in content for 2021 on the Microsoft website.

Release	Changes

2021.12.15	**All AMIs**
	• Windows Security updates current to December 14th, 2021
	• AWS Tools for Windows PowerShell version 3.15.1494
	• AWS NVMe version 1.4.0
	• SQL Server CUs installed:
	  • SQL_2017: CU 27
	  • SQL_2019: CU 13

Release	Changes
	Previous versions of Amazon-published AWS Windows AMIs dated Sep tember 15, 2021 and earlier were made private.
2021.11.16	**Windows Server 2022 and EC2Launch v1V2-* AMIs** • EC2Launch v2 version 2.0.674 Windows Server 2004 reached End-of-support on December 14, 2021. All public versions of the following images have been made private. Existing instances and custom images owned by your account that are based on Windows Server 2004 will not be impacted. • Windows_Server-2004-English-Core-Base • Windows_Server-2004-English-Core-ContainersLatest

Release	Changes
2021.11.10	**All AMIs** • Windows Security updates current to November 9th, 2021 • AWS Tools for Windows PowerShell version 3.15.1451 • AWS ENA version 2.2.4 • SQL Server CUs installed: • SQL_2017: CU 26 **New AWS Windows AMIs** • Windows_Server-2022-Japanese-Full-SQL_2019_Enterprise-2021.11.10 • Windows_Server-2022-Japanese-Full-SQL_2019_Standard-2021.11.10 • Windows_Server-2022-Japanese-Full-SQL_2019_Web-2021.11.10 • Windows_Server-2022-Japanese-Full-SQL_2017_Enterprise-2021.11.10 • Windows_Server-2022-Japanese-Full-SQL_2017_Standard-2021.11.10 • Windows_Server-2022-Japanese-Full-SQL_2017_Web-2021.11.10

Release	Changes
2021.10.13	**All AMIs** • Windows Security updates current to October 12, 2021 • AWS Tools for Windows PowerShell version 3.15.1421 • SSM version 3.1.338.0 **Windows Server 2022 and EC2Launch v1V2_Preview AMIs** • EC2Launch v2 version 2.0.651 **Windows Server 2012 RTM and R2 AMIs** • EC2Config version 4.9.4508 **New AWS Windows AMIs** • Windows_Server-2022-English-Full-SQL_2019_Enterprise-2021.10.13 • Windows_Server-2022-English-Full-SQL_2019_Standard-2021.10.13 • Windows_Server-2022-English-Full-SQL_2019_Web-2021.10.13 • Windows_Server-2022-English-Full-SQL_2019_Express-2021.10.13 • Windows_Server-2022-English-Full-SQL_2017_Enterprise-2021.10.13 • Windows_Server-2022-English-Full-SQL_2017_Standard-2021.10.13 •

Release	Changes
	Windows_Server-2022-English-Full-SQL_2017_Web-2021.10.13 • Windows_Server-2022-English-Full-SQL_2017_Express-2021.10.13 **New EC2Launch v2 AMIs** The following AMIs with EC2Launch v2 long-term support are now available . The following AMIs include EC2Launch v1 v2 as the default launch agent and will be updated with new versions each month. • EC2Launch v1V2-Windows_Server-2019-English-Full-Base-2021.10.13 • EC2Launch v1V2-Windows_Server-2019-English-Core-Base-2021.10.13 • EC2Launch v1V2-Windows_Server-2019-English-Full-ContainersLatest -2021.10.13 • EC2Launch v1V2-Windows_Server-2016-English-Full-Base-2021.10.13 • EC2Launch v1V2-Windows_Server-2016-English-Core-Base-2021.10.13 • EC2Launch v1V2-Windows_Server-2012_R2_RTM-English-Full-Base-2021 .10.13 • EC2Launch v1V2-Windows_Server-2012_RTM-English-Full-Base-2021.10 .13 EC2Launch v1V2_Preview AMIs are discontinued, and will not be update d with new versions. However, earlier versions will continue to be available until January 2022. Existing images and custom images based on EC2Launch v1V2_Preview AMIs will not be impacted, and you can continue to use them in your account. We recommend that you use the new EC2Launch v2 AMIs going forward to receive security and software updates.

Release	Changes
	Windows Server 2004 will reach End-of-support on December 14, 2021. All public versions of the following images will be made private on December 14, 2021. Existing instances and custom images owned by your account that are based on Windows Server 2004 will not be impacted. If you want to retain access to Windows Server 2004, create a custom image in your account prior to December 14th. • Windows_Server-2004-English-Core-Base • Windows_Server-2004-English-Core-ContainersLatest Previous versions of Amazon-published AWS Windows AMIs dated July 14, 2021 and earlier were made private.

Release	Changes

2021.09.15	**All AMIs**
	• Windows Security updates current to September 14, 2021
	• AWS Tools for Windows PowerShell version 3.15.1398
	• SSM version 3.1.282.0
	• SQL Server CUs installed:
	  • SQL_2019: CU12
	  • SQL_2017: CU 25
	
	Windows Server 2022 and EC2Launch v1V2_Preview AMIs
	• EC2Launch v2 version 2.0.592
	
	Windows Server 2012 RTM and R2 AMIs
	• EC2Config version 4.9.4500
	
	Previous versions of Amazon-published AWS Windows AMIs dated June 9, 2021 and earlier were made private.

Release	Changes
2021.09.01	**New AWS Windows AMIs** • Windows_Server-2022-English-Full-Base-2021.08.25 • Windows_Server-2022-English-Full-ContainersLatest-2021.08.25 • Windows_Server-2022-English-Core-Base-2021.08.25 • Windows_Server-2022-English-Core-ContainersLatest-2021.08.25 • Windows_Server-2022-Chinese_Simplified-Full-Base-2021.08.25 • Windows_Server-2022-Chinese_Traditional-Full-Base-2021.08.25 • Windows_Server-2022-Czech-Full-Base-2021.08.25 • Windows_Server-2022-Dutch-Full-Base-2021.08.25 • Windows_Server-2022-French-Full-Base-2021.08.25 • Windows_Server-2022-German-Full-Base-2021.08.25 • Windows_Server-2022-Hungarian-Full-Base-2021.08.25 • Windows_Server-2022-Italian-Full-Base-2021.08.25 • Windows_Server-2022-Japanese-Full-Base-2021.08.25 • Windows_Server-2022-Korean-Full-Base-2021.08.25 • Windows_Server-2022-Polish-Full-Base-2021.08.25 • Windows_Server-2022-Portuguese_Brazil-Full-Base-2021.08.25 • Windows_Server-2022-Portuguese_Portugal-Full-Base-2021.08.25

Release	Changes
	• Windows_Server-2022-Russian-Full-Base-2021.08.25 • Windows_Server-2022-Spanish-Full-Base-2021.08.25 • Windows_Server-2022-Swedish-Full-Base-2021.08.25 • Windows_Server-2022-Turkish-Full-Base-2021.08.25 Windows Server 2022 AMIs include EC2Launch v2 by default. For more information, see EC2Launch v2. **EC2Launch v1V2_Preview AMIs** • EC2Launch v2 version 2.0.592 Previous versions of Amazon-published AWS Windows AMIs dated May 12, 2021 and earlier were made private.

Release	Changes
2021.08.11	**All AMIs** • Windows Security updates current to August 10th, 2021 • AWS Tools for Windows PowerShell version 3.15.13571 • EC2Launch v1 version 1.3.2003411 • SSM version 3.0.1181.0 • SQL Server CUs installed: • SQL_2019: CU11 **EC2Launch v1V2_Preview AMIs** • EC2Launch v2 version 2.0.548 Previous versions of Amazon-published AWS Windows AMIs dated April 14, 2021 and earlier were made private.

Release	Changes
2021.07.14	**All AMIs** • Windows Security updates current to July 13th, 2021 • AWS Tools for Windows PowerShell version 3.15.1350 • EC2Launch v1 version 1.3.2003364 • SQL Server CUs installed: • SQL_2017: CU24
2021.07.07	**All AMIs** Out-of-band AMI release that applies the July out-of-band security update recently released by Microsoft as an additional mitigation to CVE-34527. **Note** `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers\PointAndPrint` is not defined on AWS Windows AMIs provided by AWS, which is the default state. • For more information, see CVE-2021-34527 on the Microsoft website. Previous versions of Amazon-published AWS Windows AMIs dated March 10, 2021 and earlier were made private.

Release	Changes
2021.06.09	**All AMIs** • Windows Security updates current to June 8th, 2021 • AWS Tools for Windows PowerShell version 3.15.1326 • SSM version 3.0.1124.0 **Windows Server 2012RTM/2012 R2 AMIs** • EC2Config version 4.9.4419

Release	Changes
2021.05.12	**All AMIs** • Windows Security updates current to May 11th, 2021 • AWS Tools for Windows PowerShell version 3.15.1302 • EC2Launch v1 version 1.3.2003312 • SQL Server CUs installed: • SQL_2019: CU10 • Previous versions of Amazon-published AWS Windows AMIs dated February 10, 2021 and earlier were made private. **Windows Server 2012RTM/2012 R2 AMIs** • EC2Config version 4.9.4381 • SSM version 3.0.529.0 **NVIDIA GPU AMIs** • GRID version 462.31 • Tesla version 462.31 **Radeon GPU AMIs** • Radeon version 20.10.25.04

Release	Changes
2021.04.14	**All AMIs** • Windows Security updates current to April 13th, 2021 • AWS Tools for Windows PowerShell version 3.15.1280 • AWS PV version 8.4.0 • cfn-init version 2.0.6. This package includes Microsoft Visual C++ 2015-2019 Redistributable version 14.28.29913.0 as a dependency. • AWS ENA version 2.2.3 • EC2Launch v1 version 1.3.2003284 • SQL Server CUs installed: • SQL_2017: CU23 • Previous versions of Amazon-published AWS Windows AMIs dated January 13, 2021 and earlier were made private. • **Note** Windows Server 1909 reaches End of Support on May 11, 2021. All public versions of the following images will be made private on May 11th, 2021. Existing instances and custom images owned by your account that are based on Windows Server 1909 will not be impacted. To retain access to Windows Server 1909, create a custom image in your account prior to May 11, 2021. • Windows_Server-1909-English-Core-Base •

Release	Changes
	Windows_Server-1909-English-Core-ContainersLatest **EC2Launch v1V2_Preview AMIs** • EC2Launch v2 version 2.0.285

Release	Changes

2021.03.11	**All AMIs**
	• Windows Security updates current to March 9th, 2021
	• AWS Tools for Windows PowerShell version 3.15.1248
	• cfn-init version 2.0.5. This package includes Microsoft Visual C++ 2015-2019 Redistributable version 14.28.29910.0 as a dependency.
	• EC2Launch v1 version 1.3.2003236
	• SSM Agent version 3.0.529.0
	• NVIDIA GRID version 461.33
	• SQL Server CUs installed:
	  • SQL 2016_SP2: CU16
	  • SQL 2019: CU9
	• KB4577586 update for the removal of Adobe Flash Player installed on all applicable images (Adobe Flash player is not enabled by default on all images).
	
	Note
	Amazon Root CAs have been added to the Trusted Root Certificatio n Authorities certificate store on all AMIs. For more information, see https://www.amazontrust.com/repository/#rootcas.

Release	Changes
	Windows Server 2016 and 2019 AMIs • Updated from default .NET framework versions to version 4.8. **Windows Server 2012RTM/2012 R2 AMIs** • EC2Config version 4.9.4326 • SSM Agent version 3.0.431.0

Release	Changes
2021.02.10	**All AMIs** • Windows Security updates current to February 9th, 2021 • AWS Tools for Windows PowerShell version 3.15.1224 • NVIDIA GRID version 461.09 Beginning in March 2021, AWS Windows AMIs provided by AWS include Amazon Root CAs in the certificate store to minimize potential disruptio n from the upcoming S3 and CloudFront certificate migration, which is scheduled for March 23rd, 2021. For more information, see the following: • How to Prepare for the AWS Move to Its Own Certificate Authority • [Announcement] CloudFront & S3 migrating default certificates to Amazon Trust Services March 23rd 2021 Additionally, AWS will apply "update for Removal of Adobe Flash Player" (KB4577586) to all AWS Windows AMIs in March to remove the built-in Adobe Flash player, which ended support on December 31, 2020. If your use case requires the built-in Adobe Flash player, we recommend creating a custom image based on AMIs with version 2021.02.10 or earlier. For more information about the End of Support of Adobe Flash Player, see Update on Adobe Flash Player End of Support **EC2Launch v1V2_Preview AMIs** • EC2Launch v2 version 2.0.207

Release	Changes
	New AWS Windows AMIs • Windows_Server-2016-Japanese-Full-SQL_2019_Enterprise-2021.02.10 • Windows_Server-2016-Japanese-Full-SQL_2019_Standard-2021.02.10 • Windows_Server-2016-Japanese-Full-SQL_2019_Web-2021.02.10 • Windows_Server-2019-Japanese-Full-SQL_2019_Enterprise-2021.02.10 • Windows_Server-2019-Japanese-Full-SQL_2019_Standard-2021.02.10 • Windows_Server-2019-Japanese-Full-SQL_2019_Web-2021.02.10
2021.01.13	**All AMIs** • Windows Security updates current to January 12th, 2021 • AWS Tools for Windows PowerShell version 3.15.1204 • AWS ENA version 2.2.2 • EC2Launch v1 v1 version 1.3.2003210 **Windows Server SAC/2019/2016 AMIs** • SSM Agent version 3.0.431.0

Monthly AMI updates for 2020

For more information, see Description of Software Update Services and Windows Server Update Services changes in content for 2020 on the Microsoft website.

Release	Changes
2020.12.09	**All AMIs** • Windows Security updates current to December 8th, 2020 • AWS Tools for Windows PowerShell version 3.15.1181 • All SQL Server Enterprise, Standard, and Web AMIs now include SQL Server installation media at `C:\SQLServerSetup` • EC2Launch v1 v1 version 1.3.2003189 • Previous versions of Amazon-published AWS Windows AMIs dated September 9, 2020 and earlier were made private. **Windows Server 2012/2012 R2 AMIs** • EC2Config version 4.9.4279 • SSM Agent version 2.3.871.0 **EC2Launch v1V2_Preview AMIs** • EC2Launch v2 version 2.0.160
2020.11.11	**All AMIs** • Windows Security updates current to November 10th, 2020 • AWS Tools for Windows PowerShell version 3.15.1160 • SQL Server CUs installed:

Release	Changes
	• SQL 2016 SP2: CU15 • SQL 2017: CU22 • SQL 2019: CU8 • SSM Agent version 2.3.1644.0 • EC2Launch v2 Preview AMIs: EC2Launch v1 version 2.0.153 • Previous versions of Amazon-published AWS Windows AMIs dated August 12, 2020 and earlier were made private. **New AWS Windows AMIs** • Windows_Server-20H2-English-Core-Base-2020.11.11 • Windows_Server-20H2-English-Core-ContainersLatest-2020.11.11

Release	Changes
2020.10.14	**All AMIs** • Windows Security updates current to October 13th, 2020 • AWS Tools for Windows PowerShell version 3.15.1140 • NVIDIA GRID version 452.39 • EC2Launch v2 Preview AMIs: EC2Launch v1 version 2.0.146 • AWS ENA version 2.2.1 • cfn-init version 1.4.34 • Previous versions of Amazon-published AWS Windows AMIs dated July 15, 2020 and earlier were made private.

Release	Changes
2020.9.25	A new version of Amazon Machine Images with SQL Server 2019 dated 2020.09.25 has been released. This release includes the same software components as the previous release dated 2020.09.09 but does not include CU7 for SQL 2019, which has recently been removed from public av ailability by Microsoft due to a known issue with reliability of the database snapshot feature. For more information, see the following Microsoft blog post: Cumulative update 7 for SQL Server 2019 RTM on the Microsoft website. **New AWS Windows AMIs** • Windows_Server-2016-English-Full-SQL_2019_Enterprise-2020.09.25 • Windows_Server-2016-English-Full-SQL_2019_Express-2020.09.25 • Windows_Server-2016-English-Full-SQL_2019_Standard-2020.09.25 • Windows_Server-2016-English-Full-SQL_2019_Web-2020.09.25 • Windows_Server-2019-English-Full-SQL_2019_Enterprise-2020.09.25 • Windows_Server-2019-English-Full-SQL_2019_Express-2020.09.25 • Windows_Server-2019-English-Full-SQL_2019_Standard-2020.09.25 • Windows_Server-2019-English-Full-SQL_2019_Web-2020.09.25 **EC2Launch v1V2_Preview AMIs** • EC2Launch v1V2_Preview-Windows_Server-2019-English-Full-SQL_2019 _Express-2020.09.25

Release	Changes

2020.9.9	**All AMIs**
	• Windows Security updates current to September 8th, 2020
	• AWS PV drivers version 8.3.4
	• AWS ENA version 2.2.0
	• AWS Tools for Windows PowerShell version 3.15.1110
	• SQL Server CUs installed
	  • SQL_2016_SP2: CU14
	  • SQL_2019: CU7
	• Previous versions of Amazon-published AWS Windows AMIs dated June 10, 2020 and earlier were made private.
	
	Windows Server 2016/2019/1809/1903/1909/2004 AMIs
	• EC2Launch v1 version 1.3.2003155
	• SSM Agent version 2.3.1319.0
	
	EC2Launch v1V2_Preview AMIs
	• EC2Launch v2 version 2.0.124

Release	Changes
2020.8.12	**All AMIs** • Windows Security updates current to August 11th, 2020 • AWS Tools for Windows PowerShell version 3.15.1084 • G3 AMIs: NVIDIA GRID version 451.48 • EC2Launch v2 Preview AMIs: EC2Launch v1 version 2.0.104 • SQL CUs installed • SQL_2019: CU6 • Previous versions of Amazon-published AWS Windows AMIs dated May 13, 2020 and earlier were made private.

2020.7.15	**All AMIs**
	• Windows Security updates current to July 14th, 2020
	• AWS Tools for Windows PowerShell version 3.15.1064
	• ENA version 2.1.5
	• SQL Server CUs installed
	  • SQL_2017: CU21
	  • SQL_2019: CU5
	• Previous versions of Amazon-published AWS Windows AMIs dated April 15, 2020 and earlier were made private.

Release	Changes
2020.7.01	A new version of Amazon Machine Images has been released. These images include EC2Launch v2 and serve as a functional preview of the new launch agent in advance of it being included by default on all AWS Windows AMIs currently provided by AWS later this year. Note that some SSM documents and dependent services, such as EC2 Image Builder, may require updates to support EC2 Launch v2. These updates will follow in the coming weeks. These images are not recommended for use in production environments. You can read more about EC2Launch v2 at https://aws.amazon.com/about-aws/whats-new/2020/07/introducing-ec2-launch-v2-simplify-customizing-windows-instances/ and Configure a Windows instance using EC2Launch v2. All current Windows Server AMIs will continue to be provided without changes to the current launch agent, either EC2Config (Server 2012 RTM or 2012 R2) or EC2Launch v1 v1 (Server 2016 or later), for the next several months. In the near future, all Windows Server AMIs currently provided by AWS will be migrated to use EC2Launch v2 by default as part of the monthly release. EC2Launch v1V2_Preview AMIs will be updated monthly and remain available until this migration occurs. **New AWS Windows AMIs** • EC2Launch v1V2_Preview-Windows_Server-2004-English-Core-Base-2020.06.30 • EC2Launch v1V2_Preview-Windows_Server-2019-English-Full-Base-2020.06.30 • EC2Launch v1V2_Preview-Windows_Server-2019-English-Core-Base-2020.06.30 • EC2Launch v1V2_Preview-Windows_Server-2016-English-Full-Base-2020.06.30 • EC2Launch v1V2_Preview-Windows_Server-2016-English-Core-Base-2020.06.30

Release	Changes
	• EC2Launch v1V2_Preview-Windows_Server-2012_R2_RTM-English-Full-Base-2020.06.30 • EC2Launch v1V2_Preview-Windows_Server-2012_R2_RTM-English-Core-Base-2020.06.30 • EC2Launch v1V2_Preview-Windows_Server-2012_RTM-English-Full-Base-2020.06.30 • EC2Launch v1V2_Preview-Windows_Server-2019-English-Full-SQL_2019_Express-2020.06.30 • EC2Launch v1V2_Preview-Windows_Server-2016-English-Full-SQL_2017_Express-2020.06.30
2020.6.10	**All AMIs** • Windows Security updates current to June 9th, 2020 • AWS Tools for Windows PowerShell version 3.15.1034 • cfn-init version 1.4.33 • SQL CU installed: SQL_2016_SP2: CU13
2020.5.27	**New AWS Windows AMIs** • Windows_Server-2004-English-Core-Base-2020.05.27 • Windows_Server-2004-English-Core-ContainersLatest-2020.05.27

Release	Changes
2020.5.13	**All AMIs** • Windows Security updates current to May 12th, 2020 • AWS Tools for Windows PowerShell version 3.15.1013 • EC2Launch v1 version 1.3.2003150

2020.4.15	**All AMIs**
	• Windows Security updates current to April 14th, 2020
	• AWS Tools for Windows PowerShell version 3.15.998
	• EC2Config version 4.9.4222
	• EC2Launch v1 version 1.3.2003040
	• SSM Agent version 2.3.842.0
	• SQL Server CUs installed:
	  • SQL_2017: CU 20
	  • SQL_2019: CU 4

2020.3.18	**Windows Server 2019 AMIs** Resolves an intermittent issue discovered in the 2020.3.11 release in which the Background Intelligent Transfer Service (BITS) may not start within the expected time after initial OS boot, potentially resulting in timeouts, BITS errors in the event log, or failures of cmdlets involving BITS invoked quickly after the initial boot. Other Windows Server AMIs are not affected by this issue, and their latest version remains 2020.03.11.

Release	Changes

2020.3.11	**All AMIs**
	• Windows Security updates current to March 10th, 2020
	• AWS Tools for Windows PowerShell version 3.15.969
	• EC2Config version 4.9.4122
	• EC2Launch v1 version 1.3.2002730
	• SSM Agent version 2.3.814.0
	• SQL Server CUs installed:
	  • SQL_2016_SP2: CU 12
	  • SQL_2017: CU 19
	  • SQL_2019: CU 2 not applied due to known issue with SQL Agent
	• Out of band security update (KB4551762) for server core 1909 and 1903 applied to mitigate CVE-2020-0796. Other Windows Server versions are not impacted by this issue.

Release	Changes

2020.2.12	**All AMIs**
	• Windows Security updates current to February 11th, 2020
	• AWS Tools for Windows PowerShell version 3.15.945
	• Intel SRIOV driver updates
	  • 2019/1903/1909: version 2.1.185.0
	  • 2016/1809: version 2.1.186.0
	  • 2012 R2: version 1.2.199.0
	• SQL Server CUs installed:
	  • SQL_2019: CU 1
	  • SQL_2017: CU 18
	  • SQL_2016_SP2: CU 11
	
	Windows Server 2008 SP2 and Windows Server 2008 R2
	Windows Server 2008 SP2 and Window Server 2008 R2 reached End of Support (EOS) on 01/14/20 and will no longer receive regular security updates from Microsoft. AWS will no longer publish or distribute Windows Server 2008 SP2 or Windows Server 2008 R2 AMIs. Existing 2008 SP2/R2 instances and custom AMIs in your account are not impacted, and you can continue to use them after the EOS date.
	For more information about Microsoft End of Service on AWS, including upgrade and import options, as well as a full list of AMIs that are no longer

Release	Changes
	published as of 01/14/2020, see End of Support (EOS) for Microsoft Products.
2020.1.15	**All AMIs** • Microsoft security updates current to January 14, 2020 • AWS Tools for Windows PowerShell version 3.15.925 • ENA version 2.1.4 **Windows Server 2008 SP2 and Windows Server 2008 R2** Windows Server 2008 SP2 and Window Server 2008 R2 reached End of Support (EOS) on 01/14/20 and will no longer receive regular security updates from Microsoft. AWS will no longer publish or distribute Windows Server 2008 SP2 or Windows Server 2008 R2 AMIs. Existing 2008 SP2/R2 instances and custom AMIs in your account are not impacted, and you can continue to use them after the EOS date. For more information about Microsoft End of Service on AWS, including upgrade and import options, as well as a full list of AMIs that are no longer published as of 01/14/2020, see End of Support (EOS) for Microsoft Products.

Monthly AMI updates for 2019

For more information, see Description of Software Update Services and Windows Server Update Services changes in content for 2019 on the Microsoft website.

Release	Changes
2019.12.16	

Release	Changes
	All AMIs • Microsoft security updates current to December 10, 2019 • AWS Tools for Windows PowerShell version 3.15.903 **Windows Server 2008 SP2 and Windows Server 2008 R2** Microsoft will end mainstream support for Windows Server 2008 SP2 and Windows Server 2008 R2 on January 14, 2020. On this date, AWS will no longer publish or distribute Windows Server 2008 SP2 or Windows Server 2008 R2 AMIs. Existing 2008 SP2/R2 instances and custom AMIs in your account will not be impacted and you can continue to use them after the end-of-service (EOS) date. For more information about Microsoft EOS on AWS, including upgrade and import options, along with a full list of AMIs that will no longer be published or distributed on January 14, 2020, see End of Support (EOS) for Microsoft Products.

Release	Changes
2019.11.13	**All AMIs** • AWS Tools for Windows PowerShell version 3.15.876 • Windows Security updates current to November 12th, 2019 • EC2 Config version 4.9.3865 • EC2 Launch version 1.3.2002240 • SSM Agent v2.3.722.0 Previous versions of AMIs have been marked private. **New AWS Windows AMIs** • Windows_Server-1909-English-Core-Base-2019.11.13 • Windows_Server-1909-English-Core-ContainersLatest-2019.11.13 • Windows_Server-2016-English-Full-SQL_2019_Enterprise-2019.11.13 • Windows_Server-2016-English-Full-SQL_2019_Express-2019.11.13 • Windows_Server-2016-English-Full-SQL_2019_Standard-2019.11.13 • Windows_Server-2016-English-Full-SQL_2019_Web-2019.11.13 • Windows_Server-2019-English-Full-SQL_2019_Enterprise-2019.11.13 • Windows_Server-2019-English-Full-SQL_2019_Express-2019.11.13 • Windows_Server-2019-English-Full-SQL_2019_Standard-2019.11.13 •

Release	Changes
	Windows_Server-2019-English-Full-SQL_2019_Web-2019.11.13
2019.11.05	**New AWS Windows AMIs** New SQL AMIs available: • Windows_Server-2016-English-Full-SQL_2019_Enterprise-2019.11.05 • Windows_Server-2016-English-Full-SQL_2019_Express-2019.11.05 • Windows_Server-2016-English-Full-SQL_2019_Standard-2019.11.05 • Windows_Server-2016-English-Full-SQL_2019_Web-2019.11.05 • Windows_Server-2019-English-Full-SQL_2019_Enterprise-2019.11.05 • Windows_Server-2019-English-Full-SQL_2019_Express-2019.11.05 • Windows_Server-2019-English-Full-SQL_2019_Standard-2019.11.05 • Windows_Server-2019-English-Full-SQL_2019_Web-2019.11.05

Release	Changes
2019.10.09	**All AMIs** • AWS Tools for Windows PowerShell version 3.15.846 • Windows Security updates current to October 8th, 2019 • Windows Defender platform updates current and update block via registry removed. For more information, see SFC incorrectly flags Windows Defender PowerShell module files as corrupted on the Microsoft website. **New AWS Windows AMIs** New ECS-optimized AMI available: • Windows_Server-2019-English-Core-ECS_Optimized-2019.10.09
2019.09.12	**New AWS Windows AMI** • amzn2-ami-hvm-2.0.20190618-x86_64-gp2-mono .NET Core 2.2, Mono 5.18, and PowerShell 6.2 pre-installed to run your .NET applications on Amazon Linux 2 with Long Term Support (LTS)

Release	Changes
2019.09.11	**All AMIs** • AWS PV driver version 8.3.2 • AWS NVMe driver version 1.3.2 • AWS Tools for Windows PowerShell version 3.15.826 • NLA enabled on all OS 2012 RTM to 2019 AMIs • Intel 82599 VF driver reverted to version 2.0.210.0 (Server 2016) or version 2.1.138.0 (Server 2019) due to customer reported issues. Engagement with Intel concerning these issues ongoing. • Windows Security updates current to September 10, 2019 • Windows Defender platform update blocked via registry due to SFC failures introduced by latest client. Will be reenabled when patch available. For more information, see SFC incorrectly flags Windows Defender PowerShell module files as corrupted on the Microsoft website. Platform update block: HKLM:\SOFTWARE\Microsoft\Windows Defender \Miscellaneous Configuration\PreventPlatformUpdate type=DWORD, value=1 Previous versions of AMIs have been marked private. **New AWS Windows AMIs** New STIG-compliant AMIs available: • Windows_Server-2012-R2-English-STIG-Full • Windows_Server-2012-R2-English-STIG-Core

Release	Changes
	• Windows_Server-2016-English-STIG-Full • Windows_Server-2016-English-STIG-Core • Windows_Server-2019-English-STIG-Full • Windows_Server-2019-English-STIG-Core **Windows Server 2008 R2 SP1** Includes the following updates, which are required for Microsoft Extended Security (ESU) updates. • KB4490628 • KB4474419 • KB4516655 **Windows Server 2008 SP2** Includes the following updates, which are required for Microsoft Extended Security (ESU) updates. • KB4493730 • KB4474419 • KB4517134

Release	Changes
	Note NLA is now enabled on all 2012 RTM, 2012 R2, and 2016 AMIs to increase default RDP security posture. NLA remains enabled on 2019 AMIs.
2019.08.16	**All AMIs** • Microsoft security updates current to August 13th, 2019. Includes KBs addressing CVE-2019-1181, CVE-2019-1182, CVE-2019-1222, and CVE -2019-1226. • EC2Config version 4.9.3519 • SSM Agent version 2.3.634.0 • AWS Tools for Windows PowerShell version 3.15.802 • Windows Defender platform update blocked via registry due to SFC failures introduced by update. Update will be re-enabled when new patch is available. **Note** Starting in September, NLA will be enabled on all 2012 RTM, 2012 R2, and 2016 AMIs to increase default RDP security posture.

Release	Changes
2019.07.19	**New AWS Windows AMIs** • Windows_Server-2016-English-Full-ECS_Optimized-2019.07.19 • Windows_Server-2019-English-Full-ECS_Optimized-2019.07.19
2019.07.12	**All AMIs** • Microsoft security updates current to July 9th, 2019

Release	Changes

2019.06.12	**All AMIs**
	• Microsoft security updates current to June 11th, 2019
	• AWS SDK version 3.15.756
	• AWS PV driver version 8.2.7
	• AWS NVMe driver version 1.3.1
	• The following "P3" AMIs will be renamed as "Tesla" AMIs. These AMIs will support all GPU-backed AWS instances using the Tesla driver. P3 AMIs will no longer be updated after this release and will be removed as part of our regular cycle.
	  • Windows_Server-2012-R2_RTM-English-P3-2019.06.12 replaced with Windows_Server-2012-R2_RTM-English-Tesla-2019.06.12
	  • Windows_Server-2016-English-P3-2016.06.12 replaced with Windows_Server-2016-English-Tesla-2019.06.12
	New AWS Windows AMIs
	• Windows_Server-2019-English-Tesla-2019.06.12
	Previous versions of AMIs have been marked private.

2019.05.21	**Windows Server, version 1903** • AMIs are now available

Release	Changes
2019.05.15	**All AMIs** • Microsoft security updates current to May 14th, 2019 • EC2Config version 4.9.3429 • SSM Agent version 2.3.542.0 • AWS SDK version 3.15.735
2019.04.26	**All AMIs** • Fixed AMIs for Windows Server 2019 with SQL to address edge cases where the first launch of an instance may result in Instance Impairmen t and Windows displays the message "Please wait for the User Profile Service".
2019.04.21	**All AMIs** • AWS PV Driver rollback to version 8.2.6 from version 8.3.0

Release	Changes
2019.04.10	**All AMIs** • Microsoft security updates current to April 9, 2019 • AWS SDK version 3.15.715 • AWS PV Driver version 8.3.0 • EC2Launch v1 version 1.3.2001360 **New AWS Windows AMIs** • Windows_Server-2016-English-Full-SQL_2012_SP4_Standard-2019.04.10 • Windows_Server-2016-English-Full-SQL_2014_SP3_Standard-2019.04.10 • Windows_Server-2016-English-Full-SQL_2014_SP3_Enterprise-2019.04.10
2019.03.13	**All AMIs** • Microsoft security updates current to March 12, 2019 • AWS SDK version 3.15.693 • EC2Launch v1 version 1.3.2001220 • NVIDIA Tesla driver version 412.29 for Deep Learning and P3 AMIs (https://nvidia.custhelp.com/app/answers/detail/a_id/4772) Previous versions of AMIs have been marked private

Release	Changes
2019.02.13	**All AMIs** • Microsoft security updates current to February 12, 2019 • SSM Agent version 2.3.444.0 • AWS SDK version 3.15.666 • EC2Launch v1 version 1.3.2001040 • EC2Config version 4.9.3289 • AWS PV driver 8.2.6 • EBS NVMe tool SQL 2014 with Service Pack 2 and SQL 2016 with Service Pack 1 will no longer be updated after this release.
2019.02.09	**All AMIs** • AWS Windows AMIs have been updated. New AMIs can be found with the following date versions: November "2018.11.29" December "2018.12.13" January "2019.02.09" Previous versions of AMIs have been marked private

Release	Changes
2019.01.10	**All AMIs** • Microsoft security updates current to January 10, 2019 • SSM Agent version 2.3.344.0 • AWS SDK version 3.15.647 • EC2Launch v1 version 1.3.2000930 • EC2Config version 4.9.3160 **All AMIs with SQL Server** • Latest cumulative updates

Monthly AMI updates for 2018

For more information, see Description of Software Update Services and Windows Server Update Services changes in content for 2018 on the Microsoft website.

Release	Changes
2018.12.12	**All AMIs** • Microsoft security updates current to December 12, 2018 • SSM Agent version 2.3.274.0 • AWS SDK version 3.15.629 • EC2Launch v1 version 1.3.2000760

Release	Changes
	New AWS Windows AMIs • Windows_Server-2012-R2_RTM-Japanese-64Bit-SQL_2014_SP3_Standard-2018.12.12 • Windows_Server-2012-R2_RTM-Japanese-64Bit-SQL_2014_SP3_Express-2018.12.12 • Windows_Server-2012-R2_RTM-English-64Bit-SQL_2014_SP3_Enterprise-2018.12.12 • Windows_Server-2012-R2_RTM-English-64Bit-SQL_2014_SP3_Standard-2018.12.12 • Windows_Server-2012-R2_RTM-English-64Bit-SQL_2014_SP3_Express-2018.12.12 • Windows_Server-2012-R2_RTM-English-64Bit-SQL_2014_SP3_Web-2018.12.12 • Windows_Server-2012-RTM-Japanese-64Bit-SQL_2014_SP3_Express-2018.12.12 • Windows_Server-2012-RTM-Japanese-64Bit-SQL_2014_SP3_Standard-2018.12.12 • Windows_Server-2012-RTM-Japanese-64Bit-SQL_2014_SP3_Web-2018.12.12 • Windows_Server-2012-RTM-English-64Bit-SQL_2014_SP3_Standard-2018.12.12 • Windows_Server-2012-RTM-English-64Bit-SQL_2014_SP3_Express-2018.12.12 •

Release	Changes
	Windows_Server-2012-RTM-English-64Bit-SQL_2014_SP3_Web-2018.12.12 • Windows_Server-2012-R2_RTM-Japanese-64Bit-SQL_2016_SP2_Web-2018.12.12 • Windows_Server-2012-R2_RTM-Japanese-64Bit-SQL_2016_SP2_Express-2018.12.12 • Windows_Server-2012-R2_RTM-English-64Bit-SQL_2016_SP2_Enterprise-2018.12.12 • Windows_Server-2012-R2_RTM-English-64Bit-SQL_2016_SP2_Standard-2018.12.12 • Windows_Server-2012-R2_RTM-English-64Bit-SQL_2016_SP2_Express-2018.12.12 • Windows_Server-2012-R2_RTM-English-64Bit-SQL_2016_SP2_Web-2018.12.12 • Windows_Server-2012-R2_RTM-Japanese-64Bit-SQL_2016_SP2_Standard-2018.12.12 • Windows_Server-2016-Korean-Full-SQL_2016_SP2_Standard-2018.12.12 • Windows_Server-2016-Japanese-Full-SQL_2016_SP2_Enterprise-2018.12.12 • Windows_Server-2016-Japanese-Full-SQL_2016_SP2_Web-2018.12.12 • Windows_Server-2016-English-Full-SQL_2016_SP2_Web-2018.12.12 • Windows_Server-2016-Japanese-Full-SQL_2016_SP2_Standard-2018.12.12

Release	Changes
	• Windows_Server-2016-English-Full-SQL_2016_SP2_Express-2018.12.12 • Windows_Server-2016-English-Full-SQL_2016_SP2_Standard-2018.12.12 • Windows_Server-2016-English-Core-SQL_2016_SP2_Enterprise-2018.12.12 • Windows_Server-2016-English-Core-SQL_2016_SP2_Web-2018.12.12 • Windows_Server-2016-English-Core-SQL_2016_SP2_Express-2018.12.12 • Windows_Server-2016-English-Core-SQL_2016_SP2_Standard-2018.12.12 • Windows_Server-2016-Japanese-Full-SQL_2016_SP2_Standard-2018.12.12 • Windows_Server-2016-Korean-Full-SQL_2016_SP2_Standard-2018.12.12 • Windows_Server-2019-Spanish-Full-Base-2018.12.12 • Windows_Server-2019-Japanese-Full-Base-2018.12.12 • Windows_Server-2019-Portuguese_Portugal-Full-Base-2018.12.12 • Windows_Server-2019-Chinese_Traditional-Full-Base-2018.12.12 • Windows_Server-2019-Italian-Full-Base-2018.12.12 • Windows_Server-2019-Swedish-Full-Base-2018.12.12 • Windows_Server-2019-English-Core-Base-2018.12.12 • Windows_Server-2019-Hungarian-Full-Base-2018.12.12 • Windows_Server-2019-Polish-Full-Base-2018.12.12

Release	Changes
	• Windows_Server-2019-Turkish-Full-Base-2018.12.12 • Windows_Server-2019-Korean-Full-Base-2018.12.12 • Windows_Server-2019-Dutch-Full-Base-2018.12.12 • Windows_Server-2019-German-Full-Base-2018.12.12 • Windows_Server-2019-Russian-Full-Base-2018.12.12 • Windows_Server-2019-Czech-Full-Base-2018.12.12 • Windows_Server-2019-English-Full-Base-2018.12.12 • Windows_Server-2019-French-Full-Base-2018.12.12 • Windows_Server-2019-Portuguese_Brazil-Full-Base-2018.12.12 • Windows_Server-2019-Chinese_Simplified-Full-Base-2018.12.12 • Windows_Server-2019-English-Full-HyperV-2018.12.12 • Windows_Server-2019-English-Full-ContainersLatest-2018.12.12 • Windows_Server-2019-English-Core-ContainersLatest-2018.12.12 • Windows_Server-2019-English-Full-SQL_2017_Enterprise-2018.12.12 • Windows_Server-2019-English-Full-SQL_2017_Standard-2018.12.12 • Windows_Server-2019-English-Full-SQL_2017_Web-2018.12.12 • Windows_Server-2019-English-Full-SQL_2017_Express-2018.12.12 • Windows_Server-2019-English-Full-SQL_2016_SP2_Enterprise-2018.12.12

Release	Changes
	• Windows_Server-2019-English-Full-SQL_2016_SP2_Standard-2018.12.12 • Windows_Server-2019-English-Full-SQL_2016_SP2_Web-2018.12.12 • Windows_Server-2019-English-Full-SQL_2016_SP2_Express-2018.12.12 **Updated Linux AMI** • amzn2-ami-hvm-2.0.20180622.1-x86_64-gp2-dotnetcore-2018.12.12
2018.11.28	**All AMIs** • SSM Agent version 2.3.235.0 • Changes in all power schemes to set the display to never turn off
2018.11.20	**Windows_Server-2016-English-Deep-Learning** **Windows_Server-2016-English-Deep-Learning** • TensorFlow version 1.12 • MXNet version 1.3 • NVIDIA version 392.05

Release	Changes
2018.11.19	**All AMIs** • Microsoft security updates current to November 19, 2018 • AWS SDK version 3.15.602.0 • SSM Agent version 2.3.193.0 • EC2Config version 4.9.3067 • Intel Chipset INF configurations to support new instance types **Windows Server, version 1809** • AMIs are now available.

Release	Changes
2018.10.14	**All AMIs** • Microsoft security updates current to October 9, 2018 • AWS Tools for Windows PowerShell version 3.3.365.0 • CloudFormation version 1.4.31 • AWS PV Driver version 8.2.4 • AWS PCI Serial Driver version 1.0.0.0 (support for Windows 2008R2 and 2012 on Bare Metal instances • ENA Driver version 1.5.0 **Windows Server 2016 Datacenter and Standard Editions for Nano Server** Microsoft ended mainstream support for Windows Server 2016 Datacenter and Standard Editions for Nano Server installation options as of April 10, 2018.

Release	Changes
2018.09.15	**All AMIs** • Microsoft security updates current to September 12, 2018 • AWS Tools for Windows PowerShell version 3.3.343 • EC2Launch v1 version 1.3.2000430 • AWS NVMe Driver version 1.3 0 • EC2 WinUtil Driver version 2.0.0 **Windows Server 2016 Base Nano** Access to all public versions of Windows_Server-2016-English-Nano-Base will be removed in September 2018. For more information about Nano Server lifecycle, including details on launching Nano Server as a Container, see https://learn.microsoft.com/en-us/previous-versions/windows-server/it-pro/windows-server-2016/get-started/nano-in-semi-annual-channel on the Microsoft website.

Release	Changes
2018.08.15	**All AMIs** • Microsoft security updates current to August 14, 2018 • AWS Tools for Windows PowerShell version 3.3.335 • AMIs now default to use Amazon's NTP service at IP 169.254.169.123 for time synchronization. For more information, see Set the time for your Windows instance. **Windows Server 2016 Base Nano** Access to all public versions of Windows_Server-2016-English-Nano-Base will be removed in September 2018. For more information about Nano Server lifecycle, including details on launching Nano Server as a Container, see https://learn.microsoft.com/en-us/previous-versions/windows-server/it-pro/windows-server-2016/get-started/nano-in-semi-annual-channel on the Microsoft website.
2018.07.11	**All AMIs** • Microsoft security updates current to July 10, 2018 • EC2Config version 4.9.2756 • SSM Agent 2.2.800.0
2018.06.22	**Windows Server 2008 R2** • Resolves an issue with the 2018.06.13 AMIs when changing an instance from a previous generation to a current generation (for example, M4 to M5).

Release	Changes
2018.06.13	**All AMIs** • Microsoft security updates current to June 12, 2018 • EC2Config version 4.9.2688 • SSM Agent 2.2.619.0 • AWS Tools for Windows PowerShell 3.3.283.0 • AWS NVMe driver 1.2.0 • AWS PV driver 8.2.3
2018.05.09	**All AMIs** • Microsoft security updates current to May 9, 2018 • EC2Config version 4.9.2644 • SSM Agent 2.2.493.0 • AWS Tools for Windows PowerShell 3.3.270.0 **Windows Server, version 1709 and Windows Server, version 1803** • AMIs are now available. For more information, see Windows Server version 1709 and 1803 AMIs for Amazon EC2.

Release	Changes
2018.04.11	**All AMIs** • Microsoft security updates current to April 10, 2018 • EC2Config version 4.9.2586 • SSM Agent 2.2.392.0 • AWS Tools for Windows PowerShell 3.3.256.0 • CloudFormation templates 1.4.30 • Serial INF and Intel Chipset INF configurations to support new instance types **SQL Server 2017** • Cumulative update 5 (CU5) **SQL Server 2016 SP1** • Cumulative update 8 (CU8)

Release	Changes
2018.03.24	**All AMIs** • Microsoft security updates current to March 13, 2018 • EC2Config version 4.9.2565 • SSM Agent 2.2.355.0 • AWS Tools for Windows PowerShell 3.3.245.0 • AWS PV driver 8.2 • AWS ENA driver 1.2.3.0 • Amazon EC2 Hibernate Agent 1.0 (rollback from 2.1.0 in the 2018.03.16 AMI release) • AWS EC2WinUtilDriver 1.0.1 (for troubleshooting) **Windows Server 2016** • EC2Launch v1 1.3.2000080
2018.03.16	AWS has removed all AWS Windows AMIs dated 2018.03.16 due to an issue with an unquoted path in the configuration for the Amazon EC2 Hibernate Agent.
2018.03.06	**All AMIs** • AWS PV driver 8.2.1

Release	Changes
2018.02.23	**All AMIs** • AWS PV driver 7.4.6 (rollback from 8.2 in the 2018.02.13 AMI release)
2018.02.13	**All AMIs** • Microsoft security updates current to February 13, 2018 • EC2Config version 4.9.2400 • SSM Agent 2.2.160.0 • AWS Tools for Windows PowerShell 3.3.225.1 • AWS PV driver 8.2 • AWS ENA driver 1.2.3.0 • AWS NVMe driver 1.0.0.146 • Amazon EC2 HibernateAgent 1.0.0 **Windows Server 2016** • EC2Launch v1 1.3.740
2018.01.12	**All AMIs** • Microsoft security updates current to January 9, 2018

Release	Changes
2018.01.05	**All AMIs** • Microsoft security updates current to January 2018 • Registry settings to enable mitigations for the Spectre and Meltdown exploits • AWS Tools for Windows PowerShell 3.3.215 • EC2Config version 4.9.2262

Monthly AMI updates for 2017

For more information, see Description of Software Update Services and Windows Server Update Services changes in content for 2017 on the Microsoft website.

Release	Changes
2017.12.13	**All AMIs** • Microsoft security updates current to December 12, 2017 • EC2Config version 4.9.2218 • CloudFormation templates 1.4.27 • AWS NVMe driver 1.02 • SSM Agent 2.2.93.0 • AWS Tools for Windows PowerShell 3.3.201
2017.11.29	

Release	Changes
	All AMIs • Removed components for Volume Shadow Copy Service (VSS) included in 2017.11.18 and 2017.11.19 due to a compatibility issue with Windows Backup.
2017.11.19	**All AMIs** • EC2 Hibernate Agent 1.0 (supports hibernation for Spot Instances)
2017.11.18	**All AMIs** • Microsoft security updates current to November 14, 2017 • EC2Config version 4.9.2218 • SSM Agent 2.2.64.0 • AWS Tools for Windows PowerShell 3.3.182 • Elastic Network Adapter (ENA) driver 1.08 (rollback from 1.2.2 in the 2017.10.13 AMI release) • Query for the latest AWS Windows AMI using Systems Manager Parameter Store **Windows Server 2016** • EC2Launch v1 1.3.640

Release	Changes
2017.10.13	**All AMIs** • Microsoft security updates current to October 11, 2017 • EC2Config version 4.9.2188 • SSM Agent 2.2.30.0 • CloudFormation templates 1.4.24 • Elastic Network Adapter (ENA) driver 1.2.2. (Windows Server 2008 R2 through Windows Server 2016)

Release	Changes
2017.10.04	**Microsoft SQL Server** Windows Server 2016 with Microsoft SQL Server 2017 AMIs are now public in all regions. • Windows_Server-2016-English-Full-SQL_2017_Enterprise-2017.10.04 • Windows_Server-2016-English-Full-SQL_2017_Standard-2017.10.04 • Windows_Server-2016-English-Full-SQL_2017_Web-2017.10.04 • Windows_Server-2016-English-Full-SQL_2017_Express-2017.10.04 Microsoft SQL Server 2017 supports the following features: • Machine Learning Services with Python (ML and AI) and R language support • Automatic database tuning • Clusterless Availability Groups • Runs on Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES), and Ubuntu. For more information, see Installation guidance for SQL Server on Linux on the Microsoft website. Not supported on Amazon Linux. • Windows-Linux cross-OS migrations • Resumable online index rebuild • Improved adaptive query processing •

Release	Changes
	Graph data support
2017.09.13	**All AMIs** • Microsoft security updates current to September 13, 2017 • EC2Config version 4.9.2106 • SSM Agent 2.0.952.0 • AWS Tools for Windows PowerShell 3.3.143 • CloudFormation templates 1.4.21
2017.08.09	**All AMIs** • Microsoft security updates current to August 9, 2017 • EC2Config version 4.9.2016 • SSM Agent 2.0.879.0 **Windows Server 2012 R2** • Due to an internal error, these AMIs were released with an older version of AWS Tools for Windows PowerShell, 3.3.58.0.

Release	Changes
2017.07.13	**All AMIs** • Microsoft security updates current to July 13, 2017 • EC2Config version 4.9.1981 • SSM Agent 2.0.847.0 **Windows Server 2016** • Intel SRIOV Driver 2.0.210.0

Release	Changes
2017.06.14	**All AMIs** • Microsoft security updates current to June 14, 2017 • Updates for .NET Framework 4.7 installed from Windows Update • Microsoft updates to address the "privilege not held" error using the PowerShell Stop-Computer cmdlet. For more information, see Privilege not held error on the Microsoft website. • EC2Config version 4.9.1900 • SSM Agent 2.0.805.0 • AWS Tools for Windows PowerShell 3.3.99.0 • Internet Explorer 11 for the desktop is the default, instead of the immersive Internet Explorer **Windows Server 2016** • EC2Launch v1 1.3.610
2017.05.30	The Windows_Server-2008-SP2-English-32Bit-Base-2017.05.10 AMI was updated to the Windows_Server-2008-SP2-English-32Bit-Base-2017.05.30 AMI to resolve an issue with password generation.
2017.05.22	The Windows_Server-2016-English-Full-Base-2017.05.10 AMI was updated to the Windows_Server-2016-English-Full-Base-2017.05.22 AMI after som e log cleaning.

Release	Changes
2017.05.10	**All AMIs** • Microsoft security updates current to May 9, 2017 • AWS PV Driver v7.4.6 • AWS Tools for Windows PowerShell 3.3.83.0 **Windows Server 2016** • SSM Agent 2.0.767
2017.04.12	**All AMIs** • Microsoft security updates current to April 11, 2017 • AWS Tools for Windows PowerShell 3.3.71.0 • CloudFormation templates 1.4.18 **Windows Server 2003 to Windows Server 2012** • EC2Config version 4.9.1775 • SSM Agent 2.0.761.0 **Windows Server 2016** • SSM Agent 2.0.730.0

Release	Changes
2017.03.15	**All AMIs** • Microsoft security updates current to March 14, 2017 • Current AWS Tools for Windows PowerShell • Current CloudFormation templates **Windows Server 2003 to Windows Server 2012** • EC2Config version 4.7.1631 • SSM Agent 2.0.682.0 **Windows Server 2016** • SSM Agent 2.0.706.0 • EC2Launch v1 v1.3.540
2017.02.21	Microsoft recently announced that they will not release monthly patches or security updates for the month of February. All February patches and security updates will be included in the March update. Amazon Web Services did not release updated Windows Server AMIs in February.

Release	Changes
2017.01.11	**All AMIs** • Microsoft security updates current to January 10, 2017 • Current AWS Tools for Windows PowerShell • Current CloudFormation templates **Windows Server 2003 to Windows Server 2012** • EC2Config version 4.2.1442 • SSM Agent 2.0.599.0

Monthly AMI updates for 2016

For more information, see Description of Software Update Services and Windows Server Update Services changes in content for 2016 on the Microsoft website.

Release	Changes
2016.12.14	**All AMIs** • Microsoft security updates current to December 13, 2016 • Current AWS Tools for Windows PowerShell **Windows Server 2003 to Windows Server 2012** • Released EC2Config version 4.1.1396

Release	Changes
	• Elastic Network Adapter (ENA) driver 1.0.9.0 (Windows Server 2008 R2 only) **Windows Server 2016** New AMIs available in all regions: • Windows_Server-2016-English-Core-Base **Microsoft SQL Server** All Microsoft SQL Server AMIs with the latest service pack are now public in all regions. These new AMIs replace old SQL Service Pack AMIs going forward. • Windows_Server-2008-R2_SP1-English-64Bit-SQL_2012_SP3_*edition*-2016.12.14 • Windows_Server-2012-RTM-English-64Bit-SQL_2012_SP3_*edition*-2016.12.14 • Windows_Server-2012-R2_RTM-English-64Bit-SQL_2014_SP2_*edition*-2016.12.14 • Windows_Server-2012-RTM-English-64Bit-SQL_2014_SP2_*edition*-2016.12.14 • Windows_Server-2012-R2_RTM-English-64Bit-SQL_2016_SP1_*edition*-2016.12.14 • Windows_Server-2016-English-Full-SQL_2016_SP1_*edition*-2016.12.14

Release	Changes
	SQL Server 2016 SP1 is a major release. The following features, which were previously available in Enterprise edition only, are now enabled in Standard, Web, and Express editions with SQL Server 2016 SP1: • Row-level security • Dynamic Data Masking • Change Data Capture • Database snapshot • Column store • Partitioning • Compression • In Memory OLTP • Always Encrypted
2016.11.23	**Windows Server 2003 to Windows Server 2012** • Released EC2Config version 4.1.1378 • The AMIs released this month, and going forward, use the EC2Config service to process boot-time configurations and SSM Agent to process AWS Systems Manager Run Command and Config requests. EC2Config no longer processes requests for Systems Manager Run Command and State Manager. The latest EC2Config installer installs SSM Agent side-by-side with the EC2Config service. For more information, see Configure a Windows instance using the EC2Config service (legacy).

Release	Changes
2016.11.09	**All AMIs** • Microsoft security updates current to November 8 2016 • Released AWS PV driver, version 7.4.3.0 for Windows 2008 R2 and later • Current AWS Tools for Windows PowerShell
2016.10.18	**All AMIs** • Microsoft security updates current to October 12, 2016 • Current AWS Tools for Windows PowerShell **Windows Server 2016** • Released AMIs for Windows Server 2016. These AMIs include significant changes. For example, they don't include the EC2Config service.
2016.9.14	**All AMIs** • Microsoft security updates current to September 13, 2016 • Current AWS Tools for Windows PowerShell • Renamed AMI Windows_Server-2012-RTM-Japanese-64Bit-SQL_2008_**R3_SP2**_Standard to Windows_Server-2012-RTM-Japanese-64Bit-SQL_2008_**R2_SP3**_Standard
2016.8.26	All Windows Server 2008 R2 AMIs dated 2016.08.11 were updated to fix a known issue. New AMIs are dated 2016.08.25.

Release	Changes
2016.8.11	**All AMIs** • EC2Config v3.19.1153 • Microsoft security updates current to August 10, 2016 • Enabled the registry key User32 exception handler hardening feature in Internet Explorer for MS15-124 **Windows Server 2008 R2, Windows Server 2012 RTM, and Windows Server 2012 R2** • Elastic Network Adapter (ENA) Driver 1.0.8.0 • ENA AMI property set to enabled • AWS PV Driver for Windows Server 2008 R2 was re-released this month because of a known issue. Windows Server 2008 R2 AMI's were removed in July because of this issue.
2016.8.2	All Windows Server 2008 R2 AMIs for July were removed and rolled back to AMIs dated 2016.06.15, because of an issue discovered in the AWS PV driver. The AWS PV driver issue has been fixed. The August AMI release will include Windows Server 2008 R2 AMIs with the fixed AWS PV driver and July/August Windows updates.

Release	Changes
2016.7.26	**All AMIs** • EC2Config v3.18.1118 • 2016.07.13 AMIs were missing security patches. AMIs were re-patched. Additional processes were put in place to verify successful patch installat ions going forward.
2016.7.13	**All AMIs** • Microsoft security updates current to July 2016 • Current AWS Tools for Windows PowerShell • Updated AWS PV Driver 7.4.2.0 • AWS PV Driver for Windows Server 2008 R2

Release	Changes
2016.6.16	**All AMIs** • Microsoft security updates current to June 2016 • Current AWS Tools for Windows PowerShell • EC2Config service version 3.17.1032 **Microsoft SQL Server** • Released 10 AMIs that include 64-bit versions of Microsoft SQL Server 2016. If using the Amazon EC2 console, navigate to **Images**, **AMIs**, **Public Images**, and type **`Windows_Server-2012-R2_RTM-English-64Bit-SQL_2016_Standard`** in the search bar.
2016.5.11	**All AMIs** • Microsoft security updates current to May 2016 • Current AWS Tools for Windows PowerShell • EC2Config service version 3.16.930 • MS15-011 Active Directory patch installed **Windows Server 2012 R2** • Intel SRIOV Driver 1.0.16.1

Release	Changes
2016.4.13	**All AMIs** • Microsoft security updates current to April 2016 • Current AWS Tools for Windows PowerShell • EC2Config service version 3.15.880
2016.3.9	**All AMIs** • Microsoft security updates current to March 2016 • Current AWS Tools for Windows PowerShell • EC2Config service version 3.14.786
2016.2.10	**All AMIs** • Microsoft security updates current to February 2016 • Current AWS Tools for Windows PowerShell • EC2Config service version 3.13.727
2016.1.25	**All AMIs** • Microsoft security updates current to January 2016 • Current AWS Tools for Windows PowerShell • EC2Config service version 3.12.649

Release	Changes
2016.1.5	**All AMIs** • Current AWS Tools for Windows PowerShell

Monthly AMI updates for 2015

For more information, see Description of Software Update Services and Windows Server Update Services changes in content for 2015 on the Microsoft website.

Release	Changes
2015.12.15	**All AMIs** • Microsoft security updates current to December 2015 • Current AWS Tools for Windows PowerShell
2015.11.11	**All AMIs** • Microsoft security updates current to November 2015 • Current AWS Tools for Windows PowerShell • EC2Config service version 3.11.521 • CFN Agent updated to latest version
2015.10.26	Corrected boot volume sizes of base AMIs to be 30GB instead of 35GB
2015.10.14	**All AMIs** •

Release	Changes
	Microsoft security updates current to October 2015 • EC2Config service version 3.10.442 • Current AWS Tools for Windows PowerShell • Updated SQL Service Packs to latest versions for all SQL variants • Removed old entries in Event Logs • AMI Names have been changed to reflect the latest service pack. For example, the latest AMI with Server 2012 and SQL 2014 Standard is named "Windows_Server-2012-RTM-English-64Bit-SQL_2014_SP1_Standard-2015.10.26", not "Windows_Server-2012-RTM-English-64Bit-SQL_2014_RTM_Standard-2015.10.26".
2015.9.9	**All AMIs** • Microsoft security updates current to September 2015 • EC2Config service version 3.9.359 • Current AWS Tools for Windows PowerShell • Current CloudFormation helper scripts

Release	Changes
2015.8.18	**All AMIs** • Microsoft security updates current to August 2015 • EC2Config service version 3.8.294 • Current AWS Tools for Windows PowerShell **Only AMIs with Windows Server 2012 and Windows Server 2012 R2** • AWS PV Driver 7.3.2
2015.7.21	**All AMIs** • Microsoft security updates current to July 2015 • EC2Config service version 3.7.308 • Current AWS Tools for Windows PowerShell • Modified AMI descriptions of SQL images for consistency

Release	Changes
2015.6.10	**All AMIs** • Microsoft security updates current to June 2015 • EC2Config service version 3.6.269 • Current AWS Tools for Windows PowerShell • Current CloudFormation helper scripts **Only AMIs with Windows Server 2012 R2** • AWS PV Driver 7.3.1
2015.5.13	**All AMIs** • Microsoft security updates current to May 2015 • EC2Config service version 3.5.228 • Current AWS Tools for Windows PowerShell
2015.04.15	**All AMIs** • Microsoft security updates current to April 2015 • EC2Config service version 3.3.174 • Current AWS Tools for Windows PowerShell

Release	Changes
2015.03.11	**All AMIs** • Microsoft security updates current to March 2015 • EC2Config service version 3.2.97 • Current AWS Tools for Windows PowerShell **Only AMIs with Windows Server 2012 R2** • AWS PV Driver 7.3.0
2015.02.11	**All AMIs** • Microsoft security updates current to February 2015 • EC2Config service version 3.0.54 • Current AWS Tools for Windows PowerShell • Current CloudFormation helper scripts
2015.01.14	**All AMIs** • Microsoft security updates current to January 2015 • EC2Config service version 2.3.313 • Current AWS Tools for Windows PowerShell • Current CloudFormation helper scripts

Subscribe to AWS Windows AMI notifications

Whenever AWS Windows AMIs are released, we send notifications to the subscribers of the `ec2-windows-ami-update` topic. Whenever released AWS Windows AMIs are made private, we send notifications to the subscribers of the `ec2-windows-ami-private` topic. If you no longer want to receive these notifications, use the following procedure to unsubscribe.

To be notified when new AMIs are released or when previously released AMIs are made private, subscribe to notifications using Amazon SNS.

To subscribe to AWS Windows AMI notifications

1. Open the Amazon SNS console at https://console.aws.amazon.com/sns/v3/home.
2. In the navigation bar, change the Region to **US East (N. Virginia)**, if necessary. You must use this Region because the Amazon SNS notifications that you are subscribing to were created in this Region.
3. In the navigation pane, choose **Subscriptions**.
4. Choose **Create subscription**.
5. For the **Create subscription** dialog box, do the following:
   a. For **Topic ARN**, copy and paste one of the following Amazon Resource Names (ARNs):
      - **`arn:aws:sns:us-east-1:801119661308:ec2-windows-ami-update`**
      - **`arn:aws:sns:us-east-1:801119661308:ec2-windows-ami-private`**

      For **AWS GovCloud (US) Regions**:

      `arn:aws-us-gov:sns:us-gov-west-1:077303321853:ec2-windows-ami-update`
   b. For **Protocol**, choose **Email**.
   c. For **Endpoint**, enter an email address that you can use to receive the notifications.
   d. Choose **Create subscription**.
6. You'll receive a confirmation email with the subject line `AWS Notification - Subscription Confirmation`. Open the email and choose **Confirm subscription** to complete your subscription.

To unsubscribe from AWS Windows AMI notifications

1. Open the Amazon SNS console at https://console.aws.amazon.com/sns/v3/home.
2. In the navigation bar, change the Region to **US East (N. Virginia)**, if necessary. You must use this Region because the Amazon SNS notifications were created in this Region.
3. In the navigation pane, choose **Subscriptions**.
4. Select the subscriptions and then choose **Delete**. When prompted for confirmation, choose **Delete**.

Security in AWS Windows AMI

Cloud security at AWS is the highest priority. As an AWS customer, you benefit from a data center and network architecture that is built to meet the requirements of the most security-sensitive organizations.

Security is a shared responsibility between AWS and you. The shared responsibility model describes this as security of the cloud and security in the cloud:

- **Security of the cloud** – AWS is responsible for protecting the infrastructure that runs AWS services in the AWS Cloud. AWS also provides you with services that you can use securely. Third-party auditors regularly test and verify the effectiveness of our security as part of the AWS Compliance Programs. To learn about the compliance programs that apply to Windows AMI, see AWS Services in Scope by Compliance Program.
- **Security in the cloud** – Your responsibility is determined by the AWS service that you use. You are also responsible for other factors including the sensitivity of your data, your company's requirements, and applicable laws and regulations

For detailed information about how to configure Amazon EC2 to meet your security and compliance objectives, see Security in Amazon EC2 in the *User Guide for Windows Instances*.

Document history for the AWS Windows AMI reference

The following table describes documentation changes for the AWS Windows AMI reference content. For monthly AMI version release notes, see AWS Windows AMI version history.

Change	Description	Date
Archive 2014 release notes	Yearly archive of release notes more than ten years old.	January 21, 2025
Add support for Windows Server 2025	Release AMIs for Windows Server 2025.	November 4, 2024
Initial release	Initial release of the AWS Windows AMI reference.	April 30, 2024