Manage Vscan On-Access policies

REST API reference

NetApp
February 06, 2026

This PDF was generated from https://docs.netapp.com/us-en/ontap-restapi/protocols_vscan_svm.uuid_on-access-policies_endpoint_overview.html on February 06, 2026. Always check docs.netapp.com for the latest.

Table of Contents

Manage Vscan On-Access policies . . . 1
Manage Vscan On-Access policies . . . 1
Overview . . . 1
Examples . . . 1
Retrieve a Vscan On-Access policy . . . 7
Related ONTAP commands . . . 7
Learn more . . . 7
Parameters . . . 8
Response . . . 10
Error . . . 12
Definitions . . . 12
Create a Vscan On-Access policy . . . 15
Required properties . . . 15
Default property values . . . 15
Related ONTAP commands . . . 16
Learn more . . . 16
Parameters . . . 16
Request Body . . . 16
Response . . . 18
Error . . . 19
Definitions . . . 19
Delete an antivirus On-Access policy configuration . . . 22
Related ONTAP commands . . . 22
Learn more . . . 22
Parameters . . . 22
Response . . . 22
Error . . . 22
Definitions . . . 23
Retrieve the Vscan On-Access policy configuration for an SVM . . . 24
Related ONTAP commands . . . 24
Learn more . . . 24
Parameters . . . 24
Response . . . 25
Error . . . 26
Definitions . . . 27
Update the Vscan On-Access policy configuration for an SVM . . . 29
Related ONTAP commands . . . 29
Learn more . . . 30
Parameters . . . 30
Request Body . . . 30
Response . . . 31
Error . . . 31
Definitions . . . 32

Manage Vscan On-Access policies

Manage Vscan On-Access policies

Overview

Use Vscan On-Access scanning to actively scan file objects for viruses when clients access files over SMB. To control which file operations trigger a vscan, use Vscan File-Operations Profile (vscan-fileop-profile) option in the CIFS share. The Vscan On-Access policy configuration defines the scope and status of On-Access scanning on file objects. Use this API to retrieve and manage Vscan On-Access policy configurations and Vscan On-Access policy statuses for the SVM.

Examples

Retrieving all fields for all policies of an SVM

```
# The API:
/api/protocols/vscan/{svm.uuid}/on-access-policies/

# The call:
curl -X GET "https://<mgmt-ip>/api/protocols/vscan/{svm.uuid}/on-access-
policies?fields=*" -H "accept: application/hal+json"

# The response:
{
"records": [
  {
    "svm": {
      "uuid": "179d3c85-7053-11e8-b9b8-005056b41bd1",
      "name": "vs1",
      "_links": {
        "self": {
          "href": "/api/svm/svms/179d3c85-7053-11e8-b9b8-005056b41bd1"
        }
      }
    },
    "name": "default_CIFS",
    "enabled": true,
    "mandatory": true,
    "scope": {
      "max_file_size": 2147483648,
      "include_extensions": [
        "*"
      ],
      "scan_without_extension": true,
```

```
      "scan_readonly_volumes": false,
      "only_execute_access": false
    },
    "protocol": "CIFS",
    "owner": "cluster",
    "_links": {
      "self": {
        "href": "/api/protocols/vscan/179d3c85-7053-11e8-b9b8-
005056b41bd1/on-access-policies/default_CIFS"
      }
    }
  },
  {
    "svm": {
      "uuid": "179d3c85-7053-11e8-b9b8-005056b41bd1",
      "name": "vs1",
      "_links": {
        "self": {
          "href": "/api/svm/svms/179d3c85-7053-11e8-b9b8-005056b41bd1"
        }
      }
    },
    "name": "on-access-policy",
    "enabled": false,
    "mandatory": true,
    "scope": {
      "max_file_size": 3221225472,
      "exclude_paths": [
        "\\vol\\a b\\",
        "\\vol\\a,b\\"
      ],
      "include_extensions": [
        "mp*",
        "tx*"
      ],
      "exclude_extensions": [
        "mp3",
        "txt"
      ],
      "scan_without_extension": true,
      "scan_readonly_volumes": false,
      "only_execute_access": true
    },
    "protocol": "CIFS",
    "owner": "vserver",
    "_links": {
```

```
      "self": {
        "href": "/api/protocols/vscan/179d3c85-7053-11e8-b9b8-
005056b41bd1/on-access-policies/on-access-policy"
      }
    }
  }
],
"num_records": 2,
"_links": {
  "self": {
    "href": "/api/protocols/vscan/179d3c85-7053-11e8-b9b8-005056b41bd1/on-
access-policies?fields=*"
  }
}
}
```

Retrieving the specific On-Access policy associated with the specified SVM

```
# The API:
/api/protocols/vscan/{svm.uuid}/on-access-policies/{name}

# The call:
curl -X GET "https://<mgmt-ip>/api/protocols/vscan/179d3c85-7053-11e8-
b9b8-005056b41bd1/on-access-policies/on-access-policy" -H "accept:
application/json"

# The response:
{
"svm": {
  "uuid": "179d3c85-7053-11e8-b9b8-005056b41bd1",
  "name": "vs1",
  "_links": {
    "self": {
      "href": "/api/svm/svms/179d3c85-7053-11e8-b9b8-005056b41bd1"
    }
  }
},
"name": "on-access-policy",
"enabled": true,
"mandatory": true,
"scope": {
  "max_file_size": 3221225472,
```

```
  "exclude_paths": [
    "\\vol\\a b\\",
    "\\vol\\a,b\\"
  ],
  "include_extensions": [
    "mp*",
    "tx*"
  ],
  "exclude_extensions": [
    "mp3",
    "txt"
  ],
  "scan_without_extension": true,
  "scan_readonly_volumes": false,
  "only_execute_access": true
},
"_links": {
  "self": {
    "href": "/api/protocols/vscan/179d3c85-7053-11e8-b9b8-005056b41bd1/on-
access-policies/task1"
  }
}
}
```

Creating a Vscan On-Access policy

The Vscan On-Access policy POST endpoint creates an On-Access policy for the specified SVM. Set enabled to "true" to enable scanning on the created policy.

```
# The API:
/api/protocols/vscan/{svm.uuid}/on-access-policies

# The call:
curl -X POST "https://<mgmt-ip>/api/protocols/vscan/86fbc414-f140-11e8-
8e22-0050568e0945/on-access-policies?return_records=true" -H "accept:
application/json" -H "Content-Type: application/json" -d "{ \"enabled\":
false, \"mandatory\": true, \"name\": \"on-access-policy\", \"scope\": {
\"exclude_extensions\": [ \"txt\", \"mp3\" ], \"exclude_paths\": [
\"\\\\dir1\\\\dir2\\\\ame\", \"\\\\vol\\\\a b\" ], \"include_extensions\":
[  \"mp*\", \"txt\" ], \"max_file_size\": 3221225472,
\"only_execute_access\": true, \"scan_readonly_volumes\": false,
\"scan_without_extension\": true }}"

# The response:
```

```
{
"num_records": 1,
"records": [
  {
    "svm": {
      "name": "vs1"
    },
    "name": "on-access-policy",
    "enabled": false,
    "mandatory": true,
    "scope": {
      "max_file_size": 3221225472,
      "exclude_paths": [
        "\\dir1\\dir2\\ame",
        "\\vol\\a b"
      ],
      "include_extensions": [
        "mp*",
        "txt"
      ],
      "exclude_extensions": [
        "txt",
        "mp3"
      ],
      "scan_without_extension": true,
      "scan_readonly_volumes": false,
      "only_execute_access": true
    }
  }
]
}
```


Creating a Vscan On-Access policy where a number of optional fields are not specified

```
# The API:
/api/protocols/vscan/{svm.uuid}/on-access-policies

# The call:
curl -X POST "https://<mgmt-ip>/api/protocols/vscan/86fbc414-f140-11e8-
8e22-0050568e0945/on-access-policies?return_records=true" -H "accept:
application/json" -H "Content-Type: application/json" -d "{ \"enabled\":
false, \"mandatory\": true, \"name\": \"on-access-policy\", \"scope\": {
\"exclude_paths\": [ \"\\\\vol\\\\a b\", \"\\\\vol\\\\a,b\\\\\" ],
\"max_file_size\": 1073741824, \"scan_without_extension\": true }}"

# The response:
{
"num_records": 1,
"records": [
  {
    "svm": {
      "name": "vs1"
    },
    "name": "on-access-policy",
    "enabled": false,
    "mandatory": true,
    "scope": {
      "max_file_size": 1073741824,
      "exclude_paths": [
        "\\vol\\a b",
        "\\vol\\a,b\\"
      ],
      "scan_without_extension": true
    }
  }
]
}
```

Updating a Vscan On-Access policy

The policy being modified is identified by the UUID of the SVM and the policy name.

```
# The API:
/api/protocols/vscan/{svm.uuid}/on-access-policies/{name}

# The call:
curl -X PATCH "https://<mgmt-ip>/api/protocols/vscan/86fbc414-f140-11e8-
8e22-0050568e0945/on-access-policies/on-access-policy" -H "accept:
application/hal+json" -H "Content-Type: application/json" -d "{ \"scope\":
{ \"include_extensions\": [ \"txt\" ], \"only_execute_access\": true,
\"scan_readonly_volumes\": false, \"scan_without_extension\": true }}"
```

Deleting a Vscan On-Access policy

The policy to be deleted is identified by the UUID of the SVM and the policy name.

```
# The API:
/api/protocols/vscan/{svm.uuid}/on-access-policies/{name}

# The call:
curl -X DELETE "https://<mgmt-ip>/api/protocols/vscan/86fbc414-f140-11e8-
8e22-0050568e0945/on-access-policies/on-access-policy" -H "accept:
application/hal+json"
```

Retrieve a Vscan On-Access policy

GET `/protocols/vscan/{svm.uuid}/on-access-policies`

Introduced In: 9.6

Retrieves the Vscan On-Access policy.

Related ONTAP commands

- `vserver vscan on-access-policy show`
- `vserver vscan on-access-policy file-ext-to-include show`
- `vserver vscan on-access-policy file-ext-to-exclude show`
- `vserver vscan on-access-policy paths-to-exclude show`

Learn more

- DOC /protocols/vscan/{svm.uuid}/on-access-policies

Parameters

Name	Type	In	Required	Description
protocol	string	query	False	Filter by protocol • Introduced in: 9.18
mandatory	boolean	query	False	Filter by mandatory
enabled	boolean	query	False	Filter by enabled
scope.scan_readonly_volumes	boolean	query	False	Filter by scope.scan_readonly_volumes
scope.exclude_extensions	string	query	False	Filter by scope.exclude_extensions
scope.max_file_size	integer	query	False	Filter by scope.max_file_size • Max value: 1099511627776 • Min value: 1024
scope.only_execute_access	boolean	query	False	Filter by scope.only_execute_access
scope.include_extensions	string	query	False	Filter by scope.include_extensions
scope.exclude_paths	string	query	False	Filter by scope.exclude_paths • maxLength: 255 • minLength: 1
scope.scan_without_extension	boolean	query	False	Filter by scope.scan_without_extension

Name	Type	In	Required	Description
owner	string	query	False	Filter by owner • Introduced in: 9.18
name	string	query	False	Filter by name • maxLength: 256 • minLength: 1
svm.name	string	query	False	Filter by svm.name • Introduced in: 9.16
svm.uuid	string	path	True	UUID of the SVM to which this object belongs.
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.
return_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned. • Default value: 1

Name	Type	In	Required	Description
return_timeout	integer	query	False	The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached. • Max value: 120 • Min value: 0 • Default value: 15
order_by	array[string]	query	False	Order results by specified fields and optional [asc

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
num_records	integer	Number of records
records	array[vscan_on_access]	

Example response


```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "name": "on-access-test",
      "owner": "string",
      "protocol": "string",
      "scope": {
        "exclude_extensions": [
          "mp*",
          "txt"
        ],
        "exclude_paths": [
          "\\dir1\\dir2\\name",
          "\\vol\\a b",
          "\\vol\\a,b\\"
        ],
        "include_extensions": [
          "mp*",
          "txt"
        ],
        "max_file_size": 2147483648
      },
      "svm": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      }
    }
  ]
}
```

Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


```
{
  "error": {
    "arguments": [
      {
        "code": "string",
        "message": "string"
      }
    ],
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```


Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
next	href	
self	href	

scope

Name	Type	Description
exclude_extensions	array[string]	List of file extensions for which scanning is not performed.
exclude_paths	array[string]	List of file paths for which scanning must not be performed.
include_extensions	array[string]	List of file extensions to be scanned.
max_file_size	integer	Maximum file size, in bytes, allowed for scanning.
only_execute_access	boolean	Scan only files opened with execute-access.
scan_readonly_volumes	boolean	Specifies whether or not read-only volume can be scanned.
scan_without_extension	boolean	Specifies whether or not files without any extension can be scanned.

_links

Name	Type	Description
self	href	

svm

SVM, applies only to SVM-scoped objects.

Name	Type	Description
_links	_links	
name	string	The name of the SVM. This field cannot be specified in a PATCH method.
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

vscan_on_access

An On-Access policy that defines the scope of an On-Access scan. Use On-Access scanning to check for viruses when clients open, read, rename, or close files over CIFS. By default, ONTAP creates an On-Access policy named "default_CIFS" and enables it for all the SVMs in a cluster.

Name	Type	Description
enabled	boolean	Status of the On-Access Vscan policy
mandatory	boolean	Specifies if scanning is mandatory. File access is denied if there are no external virus-scanning servers available for virus scanning.
name	string	On-Access policy name
owner	string	Specifies the on-access policy owner.
protocol	string	Specifies the file access protocol for the on-access policy. The following lists the possible protocols. CIFS - SMB protocol
scope	scope	
svm	svm	SVM, applies only to SVM-scoped objects.

error_arguments

Name	Type	Description
code	string	Argument code

Name	Type	Description
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Create a Vscan On-Access policy

POST `/protocols/vscan/{svm.uuid}/on-access-policies`

Introduced In: 9.6

Creates a Vscan On-Access policy. Important notes:

- You must enable the policy on an SVM before its files can be scanned.
- You can enable only one On-Access policy at a time on an SVM. By default, the policy is enabled on creation. * If the Vscan On-Access policy has been created successfully on an SVM but cannot be enabled due to an error, the Vscan On-Access policy configurations are saved. The Vscan On-Access policy is then enabled using the PATCH operation.

Required properties

- `svm.uuid` - Existing SVM in which to create the Vscan On-Access policy.
- `name` - Name of the Vscan On-Access policy. Maximum length is 256 characters.

Default property values

If not specified in POST, the following default property values are assigned:

- `enabled` - *true*
- `mandatory` - *true*
- `include_extensions` - *
- `max_file_size` - *2147483648*
- `only_execute_access` - *false*

- `scan_readonly_volumes` - *false*
- `scan_without_extension` - *true*
- `protocol` - *CIFS*

Related ONTAP commands

- `vserver vscan on-access-policy create`
- `vserver vscan on-access-policy enable`
- `vserver vscan on-access-policy disable`
- `vserver vscan on-access-policy file-ext-to-include add`
- `vserver vscan on-access-policy file-ext-to-exclude add`
- `vserver vscan on-access-policy paths-to-exclude add`

Learn more

- DOC /protocols/vscan/{svm.uuid}/on-access-policies

Parameters

Name	Type	In	Required	Description
return_records	boolean	query	False	The default is false. If set to true, the records are returned. • Default value:
svm.uuid	string	path	True	UUID of the SVM to which this object belongs.

Request Body

Name	Type	Description
enabled	boolean	Status of the On-Access Vscan policy
mandatory	boolean	Specifies if scanning is mandatory. File access is denied if there are no external virus-scanning servers available for virus scanning.
name	string	On-Access policy name

Name	Type	Description
owner	string	Specifies the on-access policy owner.
protocol	string	Specifies the file access protocol for the on-access policy. The following lists the possible protocols. CIFS - SMB protocol
scope	scope	
svm	svm	SVM, applies only to SVM-scoped objects.

Example request

```
{
  "name": "on-access-test",
  "owner": "string",
  "protocol": "string",
  "scope": {
    "exclude_extensions": [
      "mp*",
      "txt"
    ],
    "exclude_paths": [
      "\\dir1\\dir2\\name",
      "\\vol\\a b",
      "\\vol\\a,b\\"
    ],
    "include_extensions": [
      "mp*",
      "txt"
    ],
    "max_file_size": 2147483648
  },
  "svm": {
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  }
}
```

Response

```
Status: 201, Created
```

Name	Type	Description
num_records	integer	Number of records
records	array[vscan_on_access]	

Example response


```
{
  "num_records": 1,
  "records": [
    {
      "name": "on-access-test",
      "owner": "string",
      "protocol": "string",
      "scope": {
        "exclude_extensions": [
          "mp*",
          "txt"
        ],
        "exclude_paths": [
          "\\dir1\\dir2\\name",
          "\\vol\\a b",
          "\\vol\\a,b\\"
        ],
        "include_extensions": [
          "mp*",
          "txt"
        ],
        "max_file_size": 2147483648
      },
      "svm": {
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      }
    }
  ]
}
```

Headers

Name	Description	Type
Location	Useful for tracking the resource location	string

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
10027043	The new On-Access policy cannot be created because the SVM has reached the maximum limit of 10 On-Access policies. Delete an existing policy in order to create a new policy
10027101	The file size must be in the range 1KB to 1TB
10027107	The include extensions list cannot be empty. Specify at least one extension for inclusion
10027109	The specified CIFS path is invalid. It must be in the form "\dir1\dir2" or "\dir1\dir2\"
10027249	The On-Access policy created successfully but failed to enable the policy. The reason for enable policy operation failure might be that another policy is enabled. Disable the enabled policy and then enable the newly created policy using the PATCH operation
10027253	The number of paths specified exceeds the configured number of maximum paths. You cannot specify more than the maximum number of configured paths
10027254	The number of extensions specified exceeds the configured maximum number of extensions. You cannot specify more than the maximum number of configured extensions

Definitions

See Definitions

scope

Name	Type	Description
exclude_extensions	array[string]	List of file extensions for which scanning is not performed.
exclude_paths	array[string]	List of file paths for which scanning must not be performed.
include_extensions	array[string]	List of file extensions to be scanned.
max_file_size	integer	Maximum file size, in bytes, allowed for scanning.
only_execute_access	boolean	Scan only files opened with execute-access.
scan_readonly_volumes	boolean	Specifies whether or not read-only volume can be scanned.
scan_without_extension	boolean	Specifies whether or not files without any extension can be scanned.

href

Name	Type	Description
href	string	

_links

svm

SVM, applies only to SVM-scoped objects.

Name	Type	Description
name	string	The name of the SVM. This field cannot be specified in a PATCH method.
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

vscan_on_access

An On-Access policy that defines the scope of an On-Access scan. Use On-Access scanning to check for viruses when clients open, read, rename, or close files over CIFS. By default, ONTAP creates an On-Access policy named "default_CIFS" and enables it for all the SVMs in a cluster.

Name	Type	Description
enabled	boolean	Status of the On-Access Vscan policy
mandatory	boolean	Specifies if scanning is mandatory. File access is denied if there are no external virus-scanning servers available for virus scanning.
name	string	On-Access policy name
owner	string	Specifies the on-access policy owner.
protocol	string	Specifies the file access protocol for the on-access policy. The following lists the possible protocols. CIFS - SMB protocol
scope	scope	
svm	svm	SVM, applies only to SVM-scoped objects.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message

Name	Type	Description
target	string	The target parameter that caused the error.

Delete an antivirus On-Access policy configuration

DELETE `/protocols/vscan/{svm.uuid}/on-access-policies/{name}`

Introduced In: 9.6

Deletes the anti-virus On-Access policy configuration.

Related ONTAP commands

- `vserver vscan on-access-policy delete`

Learn more

- DOC /protocols/vscan/{svm.uuid}/on-access-policies

Parameters

Name	Type	In	Required	Description
name	string	path	True	
svm.uuid	string	path	True	UUID of the SVM to which this object belongs.

Response

```
Status: 200, Ok
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
10027034	An On-Access policy associated with a data SVM which was created by SVM owned by the cluster cannot be deleted.

Error Code	Description
10027040	An On-Access policy with a status enabled cannot be deleted. Disable the policy and then delete the policy.

Name	Type	Description
error	returned_error	

Example error


```
{
  "error": {
    "arguments": [
      {
        "code": "string",
        "message": "string"
      }
    ],
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```


Definitions

See Definitions

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Retrieve the Vscan On-Access policy configuration for an SVM

GET `/protocols/vscan/{svm.uuid}/on-access-policies/{name}`

Introduced In: 9.6

Retrieves the Vscan On-Access policy configuration of an SVM.

Related ONTAP commands

- `vserver vscan on-access-policy show`
- `vserver vscan on-access-policy file-ext-to-include show`
- `vserver vscan on-access-policy file-ext-to-exclude show`
- `vserver vscan on-access-policy paths-to-exclude show`

Learn more

- DOC /protocols/vscan/{svm.uuid}/on-access-policies

Parameters

Name	Type	In	Required	Description
name	string	path	True	
svm.uuid	string	path	True	UUID of the SVM to which this object belongs.
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

Name	Type	Description
enabled	boolean	Status of the On-Access Vscan policy
mandatory	boolean	Specifies if scanning is mandatory. File access is denied if there are no external virus-scanning servers available for virus scanning.
name	string	On-Access policy name
owner	string	Specifies the on-access policy owner.
protocol	string	Specifies the file access protocol for the on-access policy. The following lists the possible protocols. CIFS - SMB protocol
scope	scope	
svm	svm	SVM, applies only to SVM-scoped objects.

Example response


```
{
  "name": "on-access-test",
  "owner": "string",
  "protocol": "string",
  "scope": {
    "exclude_extensions": [
      "mp*",
      "txt"
    ],
    "exclude_paths": [
      "\\dir1\\dir2\\name",
      "\\vol\\a b",
      "\\vol\\a,b\\"
    ],
    "include_extensions": [
      "mp*",
      "txt"
    ],
    "max_file_size": 2147483648
  },
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  }
}
```


Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


```
{
  "error": {
    "arguments": [
      {
        "code": "string",
        "message": "string"
      }
    ],
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```


Definitions

See Definitions

scope

Name	Type	Description
exclude_extensions	array[string]	List of file extensions for which scanning is not performed.
exclude_paths	array[string]	List of file paths for which scanning must not be performed.
include_extensions	array[string]	List of file extensions to be scanned.
max_file_size	integer	Maximum file size, in bytes, allowed for scanning.
only_execute_access	boolean	Scan only files opened with execute-access.
scan_readonly_volumes	boolean	Specifies whether or not read-only volume can be scanned.
scan_without_extension	boolean	Specifies whether or not files without any extension can be scanned.

href

Name	Type	Description
href	string	

_links

Name	Type	Description
self	href	

svm

SVM, applies only to SVM-scoped objects.

Name	Type	Description
_links	_links	

Name	Type	Description
name	string	The name of the SVM. This field cannot be specified in a PATCH method.
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Update the Vscan On-Access policy configuration for an SVM

PATCH `/protocols/vscan/{svm.uuid}/on-access-policies/{name}`

Introduced In: 9.6

Updates the Vscan On-Access policy configuration and/or enables/disables the Vscan On-Access policy of an SVM. You cannot modify the configurations for an On-Access policy associated with a data SVM which was created by SVM owned by the cluster, although you can enable and disable the policy associated with cluster SVM.

Related ONTAP commands

- `vserver vscan on-access-policy modify`

- `vserver vscan on-access-policy enable`
- `vserver vscan on-access-policy disable`
- `vserver vscan on-access-policy file-ext-to-include add`
- `vserver vscan on-access-policy file-ext-to-exclude add`
- `vserver vscan on-access-policy paths-to-exclude add`
- `vserver vscan on-access-policy file-ext-to-include remove`
- `vserver vscan on-access-policy file-ext-to-exclude remove`
- `vserver vscan on-access-policy paths-to-exclude remove`

Learn more

- DOC /protocols/vscan/{svm.uuid}/on-access-policies

Parameters

Name	Type	In	Required	Description
name	string	path	True	
svm.uuid	string	path	True	UUID of the SVM to which this object belongs.

Request Body

Name	Type	Description
enabled	boolean	Status of the On-Access Vscan policy
mandatory	boolean	Specifies if scanning is mandatory. File access is denied if there are no external virus-scanning servers available for virus scanning.
owner	string	Specifies the on-access policy owner.
protocol	string	Specifies the file access protocol for the on-access policy. The following lists the possible protocols. CIFS - SMB protocol
scope	scope	

Name	Type	Description
svm	svm	SVM, applies only to SVM-scoped objects.

Example request


```
{
  "owner": "string",
  "protocol": "string",
  "scope": {
    "exclude_extensions": [
      "mp*",
      "txt"
    ],
    "exclude_paths": [
      "\\dir1\\dir2\\name",
      "\\vol\\a b",
      "\\vol\\a,b\\"
    ],
    "include_extensions": [
      "mp*",
      "txt"
    ],
    "max_file_size": 2147483648
  },
  "svm": {
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  }
}
```


Response

```
Status: 200, Ok
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
10027033	Configurations for an On-Access policy associated with a data SVM which was created by SVM owned by the cluster cannot be modified. However, the policy can be enabled or disabled.
10027046	The specified SVM is not the owner of the specified policy. Check for the correct SVM who owns the policy.
10027101	The file size must be in the range 1KB to 1TB
10027107	The include extensions list cannot be empty. Specify at least one extension for inclusion.
10027109	The specified CIFS path is invalid. It must be in the form "\dir1\dir2" or "\dir1\dir2\".
10027249	The On-Access policy updated successfully but failed to enable/disable the policy. The reason for an enable policy operation failure might be that another policy is enabled. Disable the already enabled policy and then enable the policy. The reason for a disable policy operation failure might be that Vscan is enabled on the SVM. Disable the Vscan first and then disable the policy.
10027250	The On-Access policy cannot be enabled/disabled. The reason for an enable policy operation failure might be that another policy is enabled. Disable the already enabled policy and then enable the policy. The reason for a disable policy operation failure might be that Vscan is enabled on the SVM. Disable the Vscan and then disable the policy.
10027253	The number of paths specified exceeds the configured maximum number of paths. You cannot specify more than the maximum number of configured paths.
10027254	The number of extensions specified exceeds the configured maximum number of extensions. You cannot specify more than the maximum number of configured extensions.

Definitions

See Definitions

scope

Name	Type	Description
exclude_extensions	array[string]	List of file extensions for which scanning is not performed.
exclude_paths	array[string]	List of file paths for which scanning must not be performed.
include_extensions	array[string]	List of file extensions to be scanned.
max_file_size	integer	Maximum file size, in bytes, allowed for scanning.
only_execute_access	boolean	Scan only files opened with execute-access.
scan_readonly_volumes	boolean	Specifies whether or not read-only volume can be scanned.
scan_without_extension	boolean	Specifies whether or not files without any extension can be scanned.

href

Name	Type	Description
href	string	

_links

svm

SVM, applies only to SVM-scoped objects.

Name	Type	Description
name	string	The name of the SVM. This field cannot be specified in a PATCH method.
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

vscan_on_access

An On-Access policy that defines the scope of an On-Access scan. Use On-Access scanning to check for viruses when clients open, read, rename, or close files over CIFS. By default, ONTAP creates an On-Access policy named "default_CIFS" and enables it for all the SVMs in a cluster.

Name	Type	Description
enabled	boolean	Status of the On-Access Vscan policy
mandatory	boolean	Specifies if scanning is mandatory. File access is denied if there are no external virus-scanning servers available for virus scanning.
owner	string	Specifies the on-access policy owner.
protocol	string	Specifies the file access protocol for the on-access policy. The following lists the possible protocols. CIFS - SMB protocol
scope	scope	
svm	svm	SVM, applies only to SVM-scoped objects.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message

Name	Type	Description
target	string	The target parameter that caused the error.

Copyright information

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.