

Comp-Policy_Testing

Data collected on: 10/26/2018
11:55:37 AM

General

Details

Domain	
Owner	
Created	10/10/2018 8:20:04 AM
Modified	10/26/2018 10:49:16 AM
User Revisions	0 (AD), 0 (sysvol)
Computer Revisions	119 (AD), 119 (sysvol)
Unique ID	
GPO Status	Enabled

Links

Location	Enforced	Link Status	Path
Computers	No	Enabled	Path\Computers
Notebooks	No	Enabled	Path>Notebooks

This list only includes links in the domain of the GPO.

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

Name

List of Computers

Delegation

These groups and users have the specified permission for this GPO

Name	Allowed Permissions	Inherited
List of Domain Computers with Read Permissions		
NT AUTHORITY\Authenticated Users	Read	No
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Read	No
NT AUTHORITY\SYSTEM	Edit settings, delete, modify security	No

Computer Configuration (Enabled)

Policies

Windows Settings

Security Settings

Windows Firewall with Advanced Security

Global Settings

Policy	Setting
Policy version	2.10
Disable stateful FTP	Not Configured
Disable stateful PPTP	Not Configured
IPsec exempt	Not Configured
IPsec through NAT	Not Configured
Preshared key encoding	Not Configured
SA idle time	Not Configured
Strong CRL check	Not Configured

Inbound Rules

Name	Description
LanSweeper Allowed Ports	Ports to allow Lansweeper to be able to deploy Applications, scripts, and pull Information from the endpoint
This rule may contain some elements that cannot be interpreted by current version of GPMC reporting module	
Enabled	True
Program	Any
Action	Allow
Security	Require authentication
Authorized computers	
Authorized users	
Protocol	6
Local port	135, 139, 445
Remote port	Any
ICMP settings	Any
Local scope	Any
Remote scope	Any
Profile	Domain
Network interface type	All

Service	All programs and services
Allow edge traversal	False
Group	

Connection Security Settings

Administrative Templates

Policy definitions (ADMX files) retrieved from the central store.

Network/Link-Layer Topology Discovery

Policy	Setting	Comment
--------	---------	---------

Turn on Mapper I/O (LLTDIO) driver	Enabled	
Allow operation while in domain	Enabled	
Allow operation while in public network	Disabled	
Prohibit operation while in private network	Disabled	

Policy	Setting	Comment
--------	---------	---------

Turn on Responder (RSPNDR) driver	Enabled	
Allow operation while in domain	Enabled	
Allow operation while in public network	Disabled	
Prohibit operation while in private network	Disabled	

Network/Network Connections/Windows Firewall/Domain Profile

Policy	Setting	Comment
--------	---------	---------

Windows Firewall: Allow inbound file and printer sharing exception	Enabled	
Allow unsolicited incoming messages from these IP addresses:	*	
Syntax:		
Type "*" to allow messages from any network, or else type a comma-separated list that contains any number or combination of these:		
IP addresses, such as 10.0.0.1		
Subnet descriptions, such as 10.2.3.0/24		

The string "localsubnet"

Example: to allow messages from 10.0.0.1, 10.0.0.2, and from any system on the local subnet or on the 10.3.4.x subnet, type the following in the "Allow unsolicited" incoming messages from these IP addresses":

10.0.0.1,10.0.0.2,localsubnet,10.3.4.0/24

Policy	Setting	Comment
Windows Firewall: Allow inbound remote administration exception	Enabled	
	<p>Allow unsolicited incoming messages from these IP addresses:</p> <p>Syntax:</p> <p>Type "*" to allow messages from any network, or else type a comma-separated list that contains any number or combination of these:</p> <p>IP addresses, such as 10.0.0.1</p> <p>Subnet descriptions, such as 10.2.3.0/24</p> <p>The string "localsubnet"</p> <p>Example: to allow messages from 10.0.0.1, 10.0.0.2, and from any system on the local subnet or on the 10.3.4.x subnet, type the following in the "Allow unsolicited" incoming messages from these IP addresses":</p> <p>10.0.0.1,10.0.0.2,localsubnet,10.3.4.0/24</p>	Lansweeper server IP address
Policy	Setting	Comment

Windows Firewall: Allow local port exceptions Enabled

Windows Firewall: Define inbound port exceptions Enabled

Define port exceptions:

135:TCP:Lanswper Server IP:enabled:LanSwpr EPMAP

139:TCP: Lanswper Server IP:enabled:LanSwpr NetBIOS

445:TCP: Lanswper Server IP:enabled:LanSwpr SMB

Specify the port to open or block.

Syntax:

<Port>:<Transport>:<Scope>:<Status>:<Name>

<Port> is a decimal port number

<Transport> is either "TCP" or "UDP"

<Scope> is either "*" (for all networks) or

a comma-separated list that contains

any number or combination of these:

IP addresses, such as 10.0.0.1

Subnet descriptions, such as 10.2.3.0/24

The string "localsubnet"

<Status> is either "enabled" or "disabled"

<Name> is a text string

Example:

The following definition string adds TCP port 80

to the port exceptions list and allows it to

receive messages from 10.0.0.1, 10.0.0.2, or any

system on the 10.3.4.x subnet:

80:TCP:10.0.0.1,10.0.0.2,10.3.4.0/24:enabled:Web service

Preferences

Control Panel Settings

Services

Service (Name: tmlisten)

tmlisten (Order: 1)

General

Service name	tmlisten
Action	Start service
Startup type:	Automatic
Wait timeout if service is locked:	30 seconds

Service Account

Log on service as:	<i>No change</i>
--------------------	------------------

Recovery

First failure:	Restart the service
Second failure:	<i>No change</i>
Subsequent failures:	<i>No change</i>
Reset fail count after:	0 days
Restart service after:	1 minute

Common

Options

Stop processing items on this extension if an error occurs on this item	No
Remove this item when it is no longer applied	No
Apply once and do not reapply	No

Service (Name: TmPfw)

TmPfw (Order: 2)

General

Service name	TmPfw
Action	Start service
Startup type:	Automatic
Wait timeout if service is locked:	30 seconds

Service Account

Log on service as:	<i>No change</i>
--------------------	------------------

Recovery

First failure:	Restart the service
Second failure:	<i>No change</i>
Subsequent failures:	<i>No change</i>
Reset fail count after:	0 days
Restart service after:	1 minute

Common

Options

Stop processing items on this extension if an error occurs on this item	No
Remove this item when it is no longer applied	No
Apply once and do not reapply	No

Service (Name: ntrtscan)

ntrtscan (Order: 3)

General

Service name	ntrtscan
Action	Start service
Startup type:	Automatic
Wait timeout if service is locked:	30 seconds

Service Account

Log on service as:	<i>No change</i>
--------------------	------------------

Recovery

First failure:	Restart the service
Second failure:	<i>No change</i>
Subsequent failures:	<i>No change</i>
Reset fail count after:	0 days
Restart service after:	1 minute

Common

Options

Stop processing items on this extension if an error occurs on this item	No
Remove this item when it is no longer applied	No

Apply once and do not reapply	No	
-------------------------------	----	--

Service (Name: SSDPSRV)

SSDPSRV (Order: 4)

General

Service name	SSDPSRV	
Action	Start service	
Startup type:	Automatic	
Wait timeout if service is locked:	30 seconds	

Service Account

Log on service as:	<i>No change</i>	
--------------------	------------------	--

Recovery

First failure:	Restart the service	
Second failure:	<i>No change</i>	
Subsequent failures:	<i>No change</i>	
Reset fail count after:	0 days	
Restart service after:	1 minute	

Common

Options

Stop processing items on this extension if an error occurs on this item	No	
Remove this item when it is no longer applied	No	
Apply once and do not reapply	No	

Service (Name: upnphost)

upnphost (Order: 5)

General

Service name	upnphost	
Action	Start service	
Startup type:	Automatic	
Wait timeout if service is locked:	30 seconds	

Service Account

Log on service as:	<i>No change</i>	
--------------------	------------------	--

Recovery

First failure:	Restart the service	
----------------	---------------------	--

Second failure:	<i>No change</i>
Subsequent failures:	<i>No change</i>
Reset fail count after:	0 days
Restart service after:	1 minute

Common

Options

Stop processing items on this extension if an error occurs on this item	No
Remove this item when it is no longer applied	No
Apply once and do not reapply	No

Service (Name: Winmgmt)

Winmgmt (Order: 6)

General

Service name	Winmgmt
Action	Start service
Startup type:	Automatic
Wait timeout if service is locked:	30 seconds

Service Account

Log on service as:	<i>No change</i>
--------------------	------------------

Recovery

First failure:	Restart the service
Second failure:	<i>No change</i>
Subsequent failures:	<i>No change</i>
Reset fail count after:	0 days
Restart service after:	1 minute

Common

Options

Stop processing items on this extension if an error occurs on this item	No
Remove this item when it is no longer applied	No
Apply once and do not reapply	No

Service (Name: WinRM)

WinRM (Order: 7)**General**

Service name	WinRM
Action	Start service
Startup type:	Automatic
Wait timeout if service is locked:	30 seconds

Service Account

Log on service as:	<i>No change</i>
--------------------	------------------

Recovery

First failure:	Restart the service
Second failure:	<i>No change</i>
Subsequent failures:	<i>No change</i>
Reset fail count after:	0 days
Restart service after:	1 minute

Common**Options**

Stop processing items on this extension if an error occurs on this item	No
Remove this item when it is no longer applied	No
Apply once and do not reapply	No

Service (Name: RpcSs)**RpcSs (Order: 8)****General**

Service name	RpcSs
Action	Start service
Startup type:	Automatic
Wait timeout if service is locked:	30 seconds

Service Account

Log on service as:	<i>No change</i>
--------------------	------------------

Recovery

First failure:	Restart the service
Second failure:	<i>No change</i>
Subsequent failures:	<i>No change</i>

Reset fail count after:	0 days	
Restart service after:	1 minute	

Common

Options

Stop processing items on this extension if an error occurs on this item	No	
Remove this item when it is no longer applied	No	
Apply once and do not reapply	No	

Service (Name: Imhosts)

Imhosts (Order: 9)

General

Service name	Imhosts	
Action	Start service	
Startup type:	Automatic	
Wait timeout if service is locked:	30 seconds	

Service Account

Log on service as:	<i>No change</i>	
--------------------	------------------	--

Recovery

First failure:	Restart the service	
Second failure:	<i>No change</i>	
Subsequent failures:	<i>No change</i>	
Reset fail count after:	0 days	
Restart service after:	1 minute	

Common

Options

Stop processing items on this extension if an error occurs on this item	No	
Remove this item when it is no longer applied	No	
Apply once and do not reapply	No	

User Configuration (Enabled)

No settings defined.