Network Administrator's Guide to IBM InfoSphere VDP

Contents

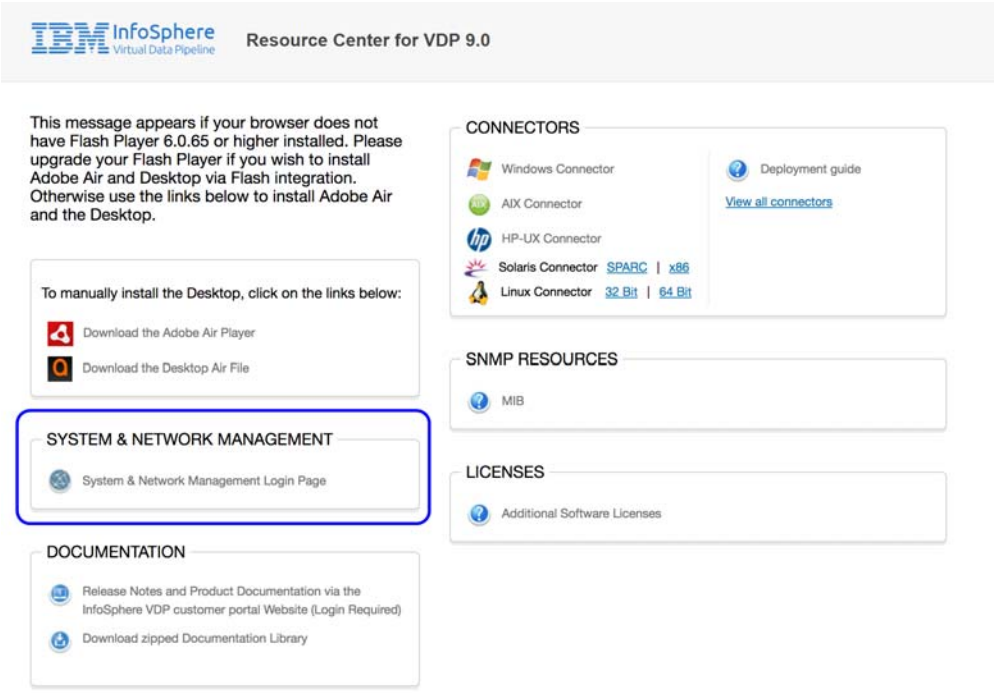
1 Modifying Your Network Configuration Settings

Your InfoSphere VDP Appliance includes a self-service network configuration feature. This document describes how to use it to:

- Modify DNS and NTP on page 2
- Modify IPs and Interfaces on page 3
- Create and modify Outbound Policies on page 5
- Perform Network Troubleshooting on page 7
- Create and modify Host Resolution on page 8
- Configure Self Service Network for IBM InfoSphere VDP Appliances in the Cloud on page 9

Accessing the Appliance System Management Tools

1. Open a browser to the Resource Center **HTTP://<appliance IP address>/**.
2. Click System & Network Management Login Page.
3. Log in using the appliance credentials. The Network Settings page opens. If your VDP Appliance is in a public cloud platform, such as AWS, GCP, or Azure, see Configure Self Service Network for IBM InfoSphere VDP Appliances in the Cloud on page 9.



Accessing the System & Network Management Tools

DNS and NTP

Enter this information:

DNS Domain: Enter the domain of the hosts connected to this appliance.

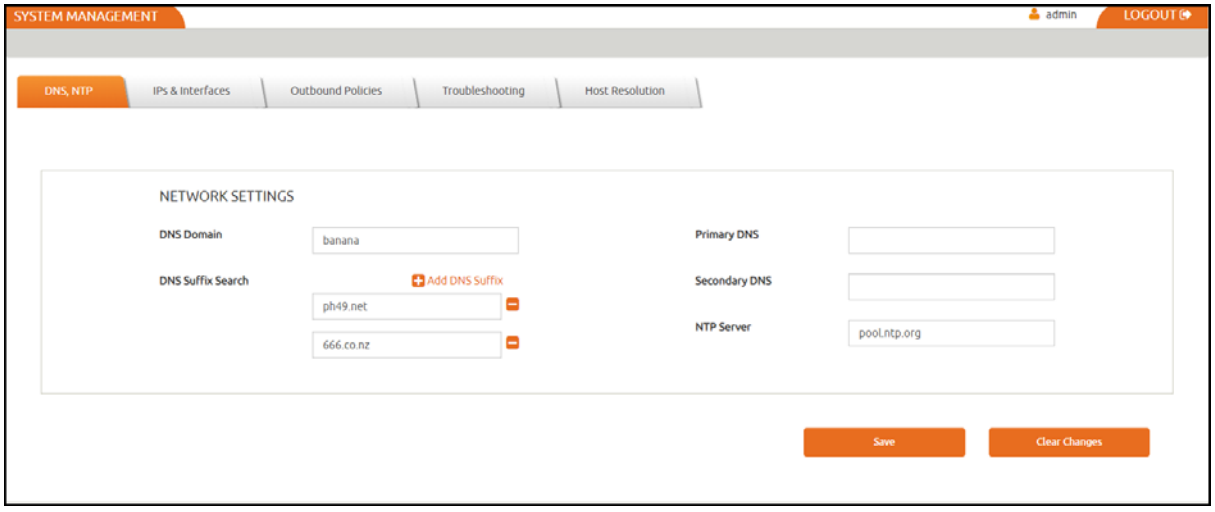
If you have additional hosts on other domains, you can set up a **DNS Suffix Search** to ensure the InfoSphere VDP Appliance can find them by their short names.

Note: *If you set any entries in DNS Suffix Search, then the DNS Domain will NOT be searched. To search both the manual entries AND the DNS domain, include the DNS domain in the DNS Suffix Search.*

Primary DNS: Enter the IP address of your primary DNS server.

Secondary DNS: Enter the IP address of your secondary DNS server (optional).

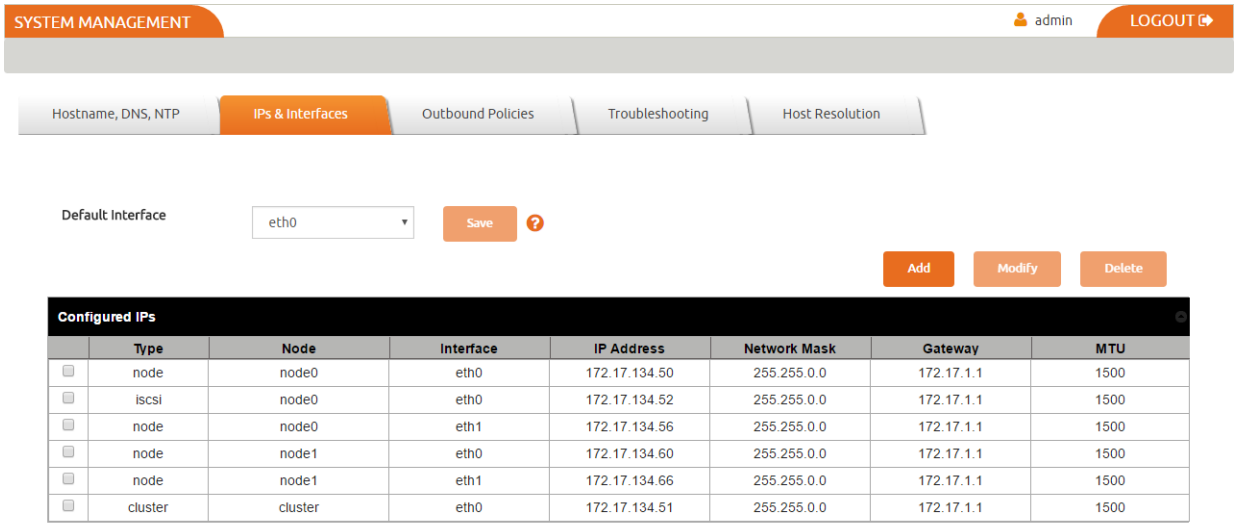
NTP Server: Enter the IP address or hostname of your NTP server.



DNS, and NTP

IPs and Interfaces

The IPs & Interfaces tab shows a list of configured IP addresses. You can modify these if necessary, and configure new interfaces added to the VDP Appliance in vCenter. The list is sorted by node first, then by interface, then by type in order (Node, iSCSI). appliance IPs are listed at the end since they are not associated with a single node. DHCP is not supported.



IPs and Interfaces

Configuring a Default Interface

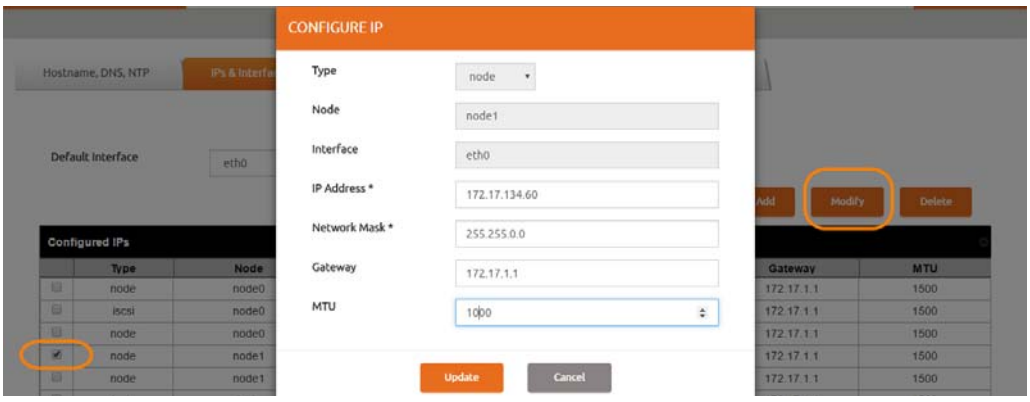
The **Default Interface** specifies which interface is used to reach arbitrary remote hosts:

- VDP Appliances always use a Node IP address.
- If no Default Interface is specified for a VDP Appliance, then the first valid Node IP address is used.

Modifying IP Address Settings

To modify a setting:

1. Check its box and click **Modify**.
2. Make your changes and click **Update**. Changes take effect immediately.



Modifying the MTU for eth0 of Node1

NIC Usage for Each InfoSphere VDP Appliance Type

InfoSphere VDP Appliances can be configured for different levels of security and availability depending on network resources. For best results, configure appliances according to the following tables:

IBM InfoSphere VDP Appliance NIC Usage on page 4

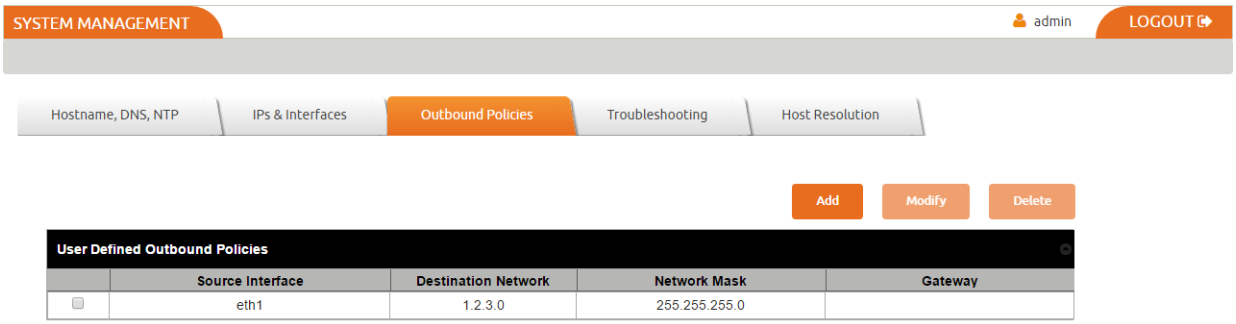
IBM InfoSphere VDP Appliance NIC Usage

Network	Security Requirement	Use
1G only virtual network	Low	Eth0 (1G) for all traffic
1/10G mixed virtual network	Medium	Eth0 (1G) for management Eth1 (1/10G) for backup/restore/replication
1/10G mixed virtual network	High	Eth0 (1G) for management Eth1 (10G) for backup Eth2 (1/10G) for replication More Eth* for backups only if required.

Outbound Policies

Outbound policies define how the InfoSphere VDP Appliance will reach specific remote networks for outbound connections. Any remote network not addressed by an outbound policy will be governed by the Default Interface configured in IPs and Interfaces on page 3.

You can also use this page to set a static route. An outbound policy is essentially a group of static routes that are automatically tailored to each of your specific interfaces.



Outbound Policies

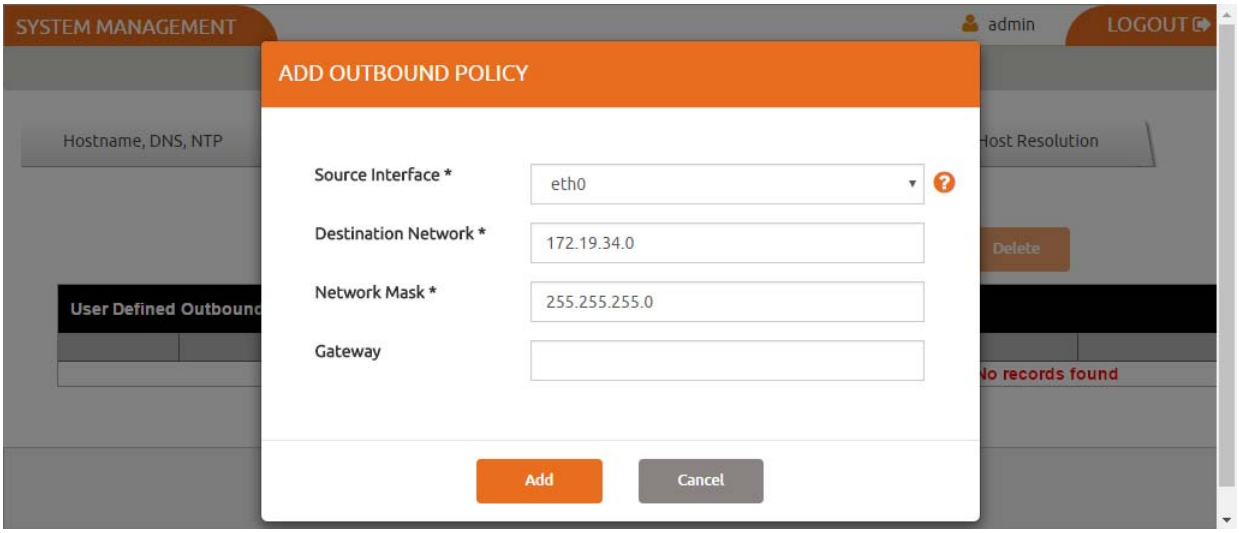
To modify an outbound policy:

1. Check its box and click **Modify**.
2. Make your changes and click **Update**. Changes take effect immediately.

To add a new outbound policy:

1. Click **Add**.
2. Enter your information and click **Add**. Changes take effect immediately.

A Gateway setting is optional. If you do not assign a gateway, then the default gateway for the interface is used. If your traffic must traverse a non-default gateway, then assign that gateway here. This gateway will be installed on every interface where it fits the netmask.



Adding an Outbound Policy

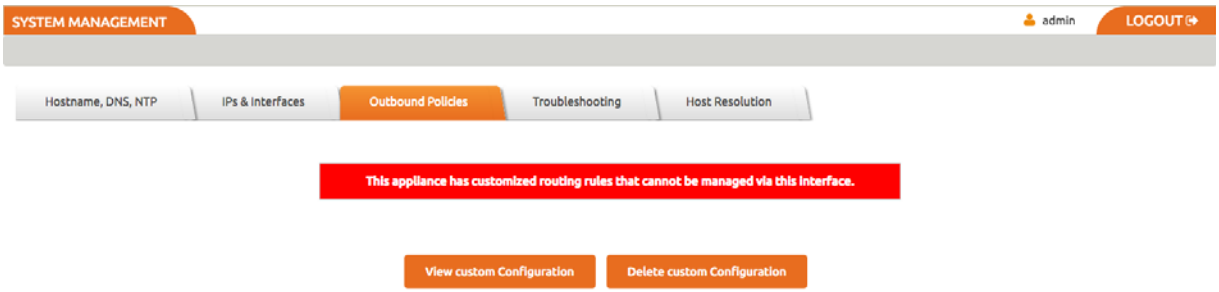
Outbound Policies and Custom Configurations

If this system has some custom networking configured by IBM InfoSphere Support, then the View and Delete Custom Configuration buttons appear on this page. You can view the text of the custom networking configuration file here.

Note: *These buttons are not visible if your appliance has never had a custom configuration. A custom configuration can be created/modified only by IBM InfoSphere Support. If you cannot make modifications to this page, it means that this system has some custom networking configured by IBM InfoSphere Support. Contact IBM InfoSphere Support for guidance.*

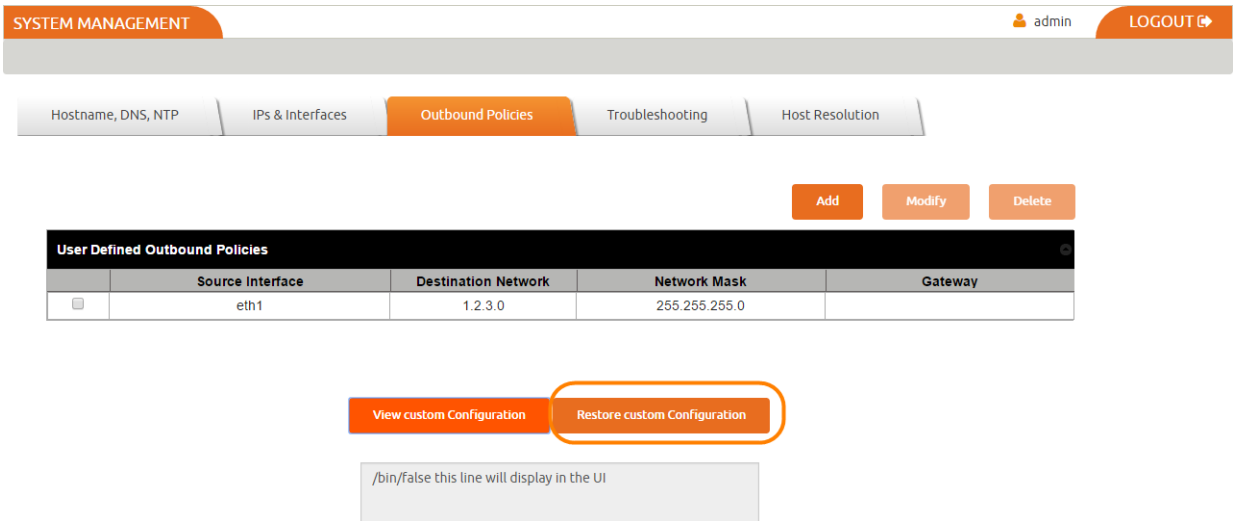
If the appliance has an active custom configuration, then you see a Delete option. This disables the custom part of the configuration, allowing you to proceed with the formerly disabled management functions.

Note: *Disabling a custom configuration may make the appliance unreachable.*



This Appliance has a Custom Configuration

If you want to reactivate your custom configuration, use the **Restore Custom Configuration** button.



Restoring a Custom Configuration

Network Troubleshooting

Use this page to troubleshoot problematic network connections. Under **Utility**, select the troubleshooting tool to use, enter the necessary parameters, and then click **Run Test**. The results appear in the Test Results box.

Ping: Runs a ping to determine reachability of a target host, returning the output as a plain text stream. This command sends 3 ICMP echo packets.
Enter:

- **Source IP**: Select the IP address of the appliance to test. This tests the behavior of a reply packet. If you do not enter a value here, then the Outbound Policy rules are used. This tests the behavior of outbound connections.
- **Destination IP**: A valid IPv4 or IPv6 address.

Example Ping result:

```
PING 1.2.3.4 (1.2.3.4) 56(84) bytes of data.
--- 1.2.3.4 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 3001ms
```

IP route get: Queries the routing tables for the selected Destination IP address without sending any packets. Enter:

- **Source IP**: Select the IP address of the appliance to test. This tests the behavior of a reply packet. If enter no value, then Outbound Policy rules are used to test the behavior of outbound connections.
- **Destination IP**: The IP address of a target host.

Example IP route get result:

```
test/routeget 1.2.3.4
1.2.3.4 via 172.17.1.2 dev eth0 src 172.17.134.80
cache mtu 1500 advmss 1460 hoplimit 64
```

Traceroute: Runs a traceroute to the given IP address by sending a series of UDP probes, returning the output as a plain text stream. This can take 30 or more seconds to run. Use Traceroute to identify intervening networks on the path. Traceroute cannot accept a source IP parameter, so it is not useful for testing the behavior of reply packets. Only outgoing connections can be diagnosed with this tool.

- **Destination IP**: The IP address of a target host.
- **UDP Port**: See Chapter 3, Firewall Rules

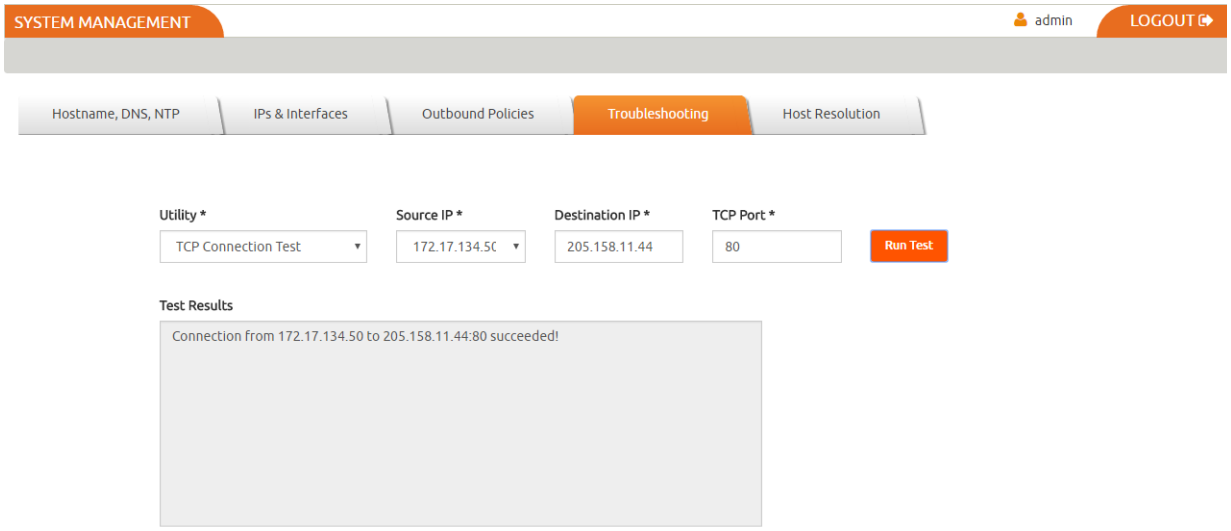
Example Traceroute result:

```
test/traceroute 8.8.8.8
1: dev134-86.dev.acme.com (172.17.134.86) 0.092ms pmtu 1500
1: devgw-waln5k02.dev.acme.com (172.17.0.3) 4.287ms
1: devgw-waln5k02.dev.acme.com (172.17.0.3) 1.287ms
2: e-1-20-walpalo.core.acme.com (192.168.255.21) 2.805ms
3: ge-0-0-1-walasr.edge.acme.com (192.43.242.209) 2.769ms
4: 205.158.44.81.ptr.us.xo.net (205.158.44.81) 9.247ms asymm 14
5: vb1020.rar3.nyc-ny.us.xo.net (216.156.0.25) 10.080ms asymm 12
6: 207.88.12.104.ptr.us.xo.net (207.88.12.104) 8.537ms asymm 12
7: 207.88.13.35.ptr.us.xo.net (207.88.13.35) 8.175ms asymm 11
8: no reply
9: no reply
.
.
.
31: no reply
Too many hops: pmtu 1500
Resume: pmtu 1500
```

TCP Connection Test: Attempts a TCP connection to the target IP and port. If successful, the connection is closed immediately without transferring any data. If not successful it returns a failure message.

- **Source IP**: Select the IP address of the appliance to test. This tests the behavior of a reply packet. If you do not enter a value here, then the Outbound Policy rules are used. This tests the behavior of outbound connections.
- **Destination IP**: The IP address of a target host.
- **TCP Port**: See Chapter 3, Firewall Rules.

Example TCP Connection Test result:



Troubleshooting: TCP Connection Test

Host Resolution

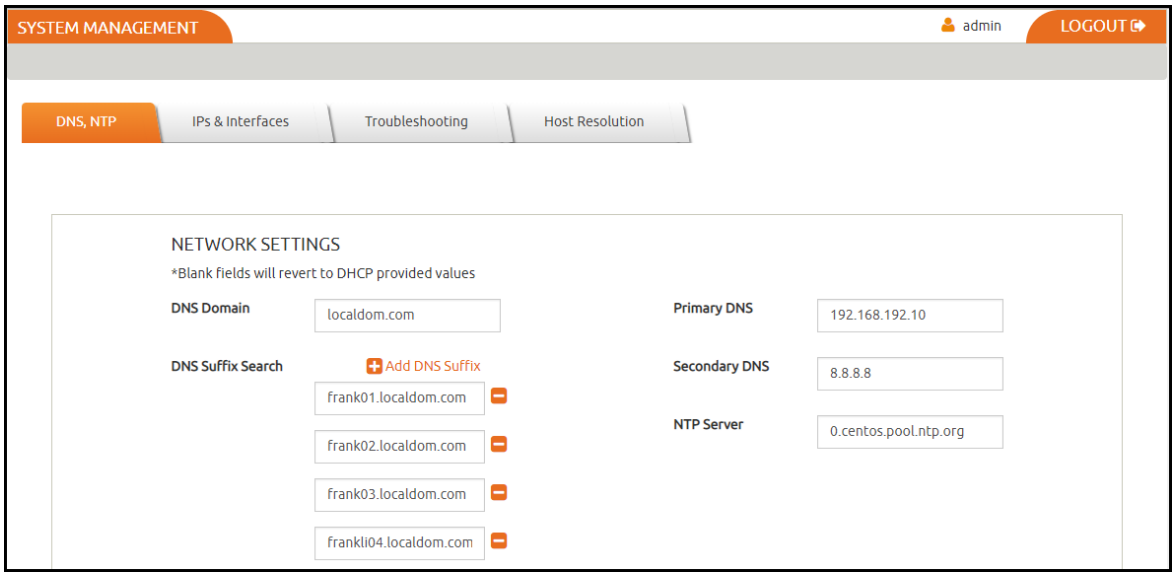
A host that has both management and production IP addresses may be configured with only the IP address for the management NIC in DNS. Use this page to add the NIC used for production communications. The information that you enter here becomes the contents of /etc/hosts.

Note you cannot define a single hostname with multiple IP addresses, as the Management Panel will not allow you to do this. Even if it allowed more than one IP address to be added for the same hostname, only the first IP address would ever be used as this how name resolution with the /etc/hosts file works (which is the reason the panel blocks attempts to add the same hostname). For the scenario where a single hostname needs to resolve to more than IP, you must rely on an external DNS to do this resolution.

Host Resolution

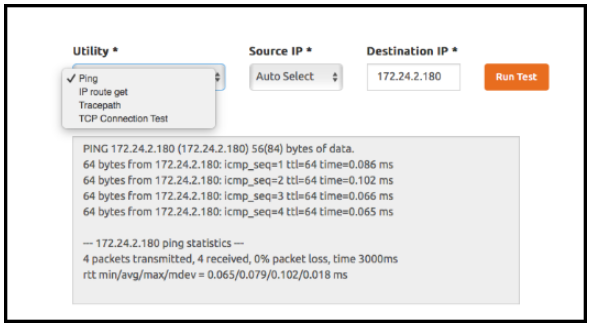
Configure Self Service Network for IBM InfoSphere VDP Appliances in the Cloud

For InfoSphere VDP Appliances on the Cloud, once you login to the System Management you will see the **DNS, NTP** tab.



System Management Tool for InfoSphere VDP Appliance on Cloud

3. Enter or modify the network settings using information in DNS and NTP on page 2. Any field you leave empty will revert to DHCP provided values.
4. Click the **IP & Interfaces** tab to view the a list of configured IP addresses. You cannot edit any information, it is view only. For more information, see IPs and Interfaces on page 3.
5. Click the **Troubleshooting** tab and troubleshoot problematic network connections using information in Network Troubleshooting on page 7.



Network Troubleshooting

6. Click the **Host Resolution tab** to override DNS resolution for specific hosts. For more information, see Host Resolution on page 8.

Note: *For appliances on the Cloud, you will not see the* ***Outbound Policies*** *tab.*

---

2 Reference Architectures for InfoSphere VDP Appliances

InfoSphere VDP Appliances can be configured for different levels of security and high availability depending on available network resources. For best results, appliances should be configured according to the following table:

IBM InfoSphere VDP Appliance Reference Architectures

VDP	Using	Network	Security	High Availability
VDP-1	Eth0 (1G) for all traffic	1G only virtual network	Low	The VDP Appliance uses the hypervisor's High Availability features.
VDP-2	Eth0 (1G) for management Eth1 (1/10G) for backup/restore/ replication	1/10G mixed virtual network	Medium	
VDP-4	Eth0 (1G) for management Eth1 (10G) for backup Eth2 (1/10G) for replication More Eth* for backups only if required.	1/10G mixed virtual network	High	

3 Firewall Rules

This section opens with an overview of Internet Protocol (IP) Network Security in an IBM InfoSphere Environment.

Then it details the network ports employed within a fully functional IBM InfoSphere copy data management environment:

Internet Protocol (IP) Network Security in an IBM InfoSphere Environment

All components of IBM InfoSphere Virtual Data Pipeline have been designed from the ground up with security in mind and the IP interfaces as traditional attack vectors have been given particular focus in hardening efforts.

Appliance Outbound Connections

The appliance may make outbound connections to the following services, but does not listen on or run a service for these ports unless listed in IBM InfoSphere Local Management from Administrator Workstation on page 14.

SNMP

For the most part SNMP code on an InfoSphere VDP Appliance is outgoing only, sending traps to a configured receiver to notify of events and failures.

A list of whitelisted IPs can be viewed with the commands `udsinfo lsmonitoreddevice`. SNMP v1 and v2 are supported.

No IBM InfoSphere configuration can accept any SNMP walk or write (e.g. GetRequest, SetRequest, GetNextRequest, GetBulkRequest) and this configuration of community names is not required or supported.

Cross Appliance Communication and Replication

All InfoSphere VDP Appliances utilize strong mutual authentication of the partner appliance with verification of 2048-bit RSA public keys.

Once authenticated, data in flight between appliances is encrypted using 256-bit AES encryption with session keys protected by Diffie-Hellman algorithms affording Perfect Forward Secrecy (PFS) over a TLS v1.2 channel.

IBM InfoSphere Local Management from Administrator Workstation

Destination Port	Protocol(s)	Source IP Address	Destination IP Address	Description
22 (TCP)	SSH	Admin workstation	InfoSphere VDP Appliance IP address IBM InfoSphere IMM Addresses	CLI access for management and backup commands. Hosts may also need to connect to IBM InfoSphere. Node IMM Ports for installation and service
26 (TCP)	SSH	Admin workstation	InfoSphere VDP Appliance IP address	Service CLI access.
80 (TCP) or 443 (TCP)	HTTP HTTPS	Admin workstation	IBM InfoSphere IMM Addresses	Node IMM Ports for installation and service. Enables local download of the VDP Desktop and Connector software. No appliance control or data access is possible on this port.
443 (TCP)	HTTPS	Admin workstation	InfoSphere VDP Appliance IP address	Provides TLS-encrypted communication between VDP Desktop clients and the appliance, as well as some appliance-to-appliance communication. SSL certificates may be customer replaced.
3900 (TCP)	HTTP	Admin workstation	IBM InfoSphere IMM Addresses	Node IMM ports for remote access

InfoSphere VDP Appliance Local Services

Destination Port	Protocol(s)	Source IP Address	Destination IP Address	Description
25 (TCP) or 465 (TCP)	SMTP SMTPS	InfoSphere VDP Appliance IP address	Client email server	Event notification via your SMTP email relay server.
53 (UDP)	DNS	InfoSphere VDP Appliance IP address	Client DNS server	DNS
123 (UDP)	NTP	InfoSphere VDP Appliance IP address	Client NTP server	NTP
162 (UDP)	SNMP	InfoSphere VDP Appliance IP address	Client SNMP server	SNMP trap notification
389 (TCP) or 636 (TCP)	LDAP LDAPS	InfoSphere VDP Appliance IP address	Client AD server and LDAP	Authentication of user accounts against a central Microsoft AD/ LDAP directory if configured.

Management Traffic to and from the InfoSphere VDP Appliance

Destination Port	Protocol(s)	Source IP Address	Destination IP Address	Description
26 (TCP)	SSH	InfoSphere VDP Appliance IP address	InfoSphere VDP Appliance IP address	Appliance to appliance cross-node management. Node addresses should also be allowed.
443 (TCP)	HTTPS	InfoSphere VDP Appliance IP address	vCenter Server IP	Required to communicate with vCenter servers and ESX hosts for snapshot and image management during backup and mounts over an encrypted link. Used for joining InfoSphere VDP Appliances and sharing certificates.
5106 (TCP)	IBM InfoSphere API	InfoSphere VDP Appliance IP address	Host Servers, including Hyper-V Host Servers	Encrypted control channel between InfoSphere VDP Appliance and hosts running the VDP Connector.

Backup Traffic from the InfoSphere VDP Appliance and Replication Traffic Between Appliances

Destination Port	Protocol(s)	Source IP Address	Destination IP Address	Description
443 (TCP)	HTTPS	InfoSphere VDP Appliance IP address	Amazon S3 Endpoint Other Appliance	IBM InfoSphere OnVault cloud data transfer Appliance-to-appliance traffic
902 (TCP)	VMware	InfoSphere VDP Appliance IP address	ESX Server VMKernel IPs	Encrypted connectivity to VMware ESXi hosts for data movement operations.
3205 and 3260 (TCP)	iSCSI	Host servers	IBM InfoSphere iSCSI Addresses	iSCSI target
111 756 2049 4001 4045	tcp/udp tcp/udp tcp/udp tcp/udp tcp/udp	InfoSphere VDP Appliance IP address	Host servers	An RPC service used to map other RPC services Network status monitor daemon NFS server process NFS mount daemon Network lock daemon
5103	IBM InfoSphere API	InfoSphere VDP Appliance IP address	Host servers	Encrypted bidirectional appliance-to-appliance data replication traffic. Both sides use strong mutual authentication of the partner appliance.
5107 (TCP)	IBM InfoSphere API	InfoSphere VDP Appliance IP address	Host servers	InfoSphere VDP Appliance to appliance data transfer for cross-site mirroring and for IBM InfoSphere StreamSnap data replication. Must be bidirectional.
5108 (TCP)	IBM InfoSphere API	InfoSphere VDP Appliance IP address	Host servers	Please keep this port open for a planned StreamSnap feature.

IBM InfoSphere Remote Support

Destination Port	Protocol	Source IP Address	Destination IP Address	Description
443 (TCP)	HTTPS	InfoSphere VDP Appliance IP address	callhome.actifio.net	Call Home Alerting

IBM InfoSphere Remote Support

Destination Port	Protocol	Source IP Address	Destination IP Address	Description
25 (TCP)	SMTP	InfoSphere VDP Appliance IP address	callhome.actifio.net	Call Home Alerting (legacy)
443 (TCP)	OpenVPN/ HTTPS	InfoSphere VDP Appliance IP address	secureconnect2.actifio.com	SecureConnect proxy mode (optional)
1194 (UDP)	OpenVPN	**VDP Appliance**: VDP Appliance IP	secureconnect2.actifio.com	SecureConnect. Encrypted remote support access to IBM InfoSphere data centers. As the connection is mutually authenticated with strong cryptography, it is recommended that the destination not be limited by a firewall.

IBM InfoSphere Report Manager

Destination Port	Protocol	Source IP Address	Destination IP Address	Description
443 (TCP)	HTTPS	Administrator workstation	Report Manager server	IBM InfoSphere Report Manager (reports & setup/ admin)
5103 (TCP) Use 443 if the firewall blocks outbound traffic	SSH	Report Manager server	InfoSphere VDP Appliance IP address	IBM InfoSphere Report Manager (data collection)

InfoSphere VDP - Global Manager (IVGM)

Destination Port	Protocol(s)	Source IP Address	Destination IP Address	Description
5103 (TCP) Use 443 if the firewall blocks outbound traffic	SSH	IVGM server	InfoSphere VDP Appliance IP address	Outbound connection from IVGM to all managed InfoSphere VDP Appliances. Once the connection is established, data flow is bidirectional.
443 (TCP)	HTTPS	Workstation or laptop	IVGM server	Web browser access to IVGM for inbound connection to IVGM server.
TCP-389 (TCP) or TCP-636 (TCP)	LDAP LDAPS	IVGM server	Client AD server	Microsoft AD/LDAP Active Directory Authentication

InfoSphere VDP Appliance IP address

InfoSphere VDP Appliance IP address is assigned at installation of the VMware or Hyper-V VM.

4 iSCSI Connectivity

This includes:

Note: *For best iSCSI network traffic results, see* NIC Usage for Each InfoSphere VDP Appliance Type *on page 4.*

Ensuring iSCSI Connectivity from ESX to Storage

Ensuring SAN transport of data to an external storage pool

A newly created vCenter will default to Transport Type NFS. This is incompatible with ESP, and should be changed to SAN. This setting is visible in IVGM and from the Command Line, but is not displayed in the VDP Desktop.

You can also do this from the CLI:

```
[root@sky812-900-RC2 ~]# udsinfo lshost 207823
...
udstask chhost -transport san <id>'\
```

The -transport parameter is detailed in the ***VDP CLI Reference***.

Ensuring iSCSI Connectivity with an ESX Server

This has two parts:

1. Adding the iSCSI IBM InfoSphere Definition to the ESX server on page 20
2. Configuring IVGM to See the ESX Host on page 21

Before You Begin

In order to ensure connectivity to ESX servers reached via iSCSI:

- Check that the NICs are as described in NIC Usage for Each InfoSphere VDP Appliance Type on page 4.
- Check that the network ports are as described in Chapter 3, Firewall Rules.
- Check each ESX server to be sure that these are set to the following recommended values:

Setting	Recom. Value	Description
LoginTimeout	60	When iSCSI establishes a session between initiator and target, it must log into the target. It will try to log in for a period of LoginTimeout. If the login attempt exceeds LoginTimeout, then the login fails.
Noopinterval	30	iSCSI uses the noop timeout to passively discover if this path is dead when it is not the active path.
Nooptimeout	30	This is tested on non-active paths every NoopInterval. If no response is received by NoopTimeout, the path is marked dead.

This procedure is for a single IBM InfoSphere Ethernet iSCSI connection to a single iSCSI Ethernet connection on the ESX server. IBM InfoSphere Professional Services can help you with any other configuration.

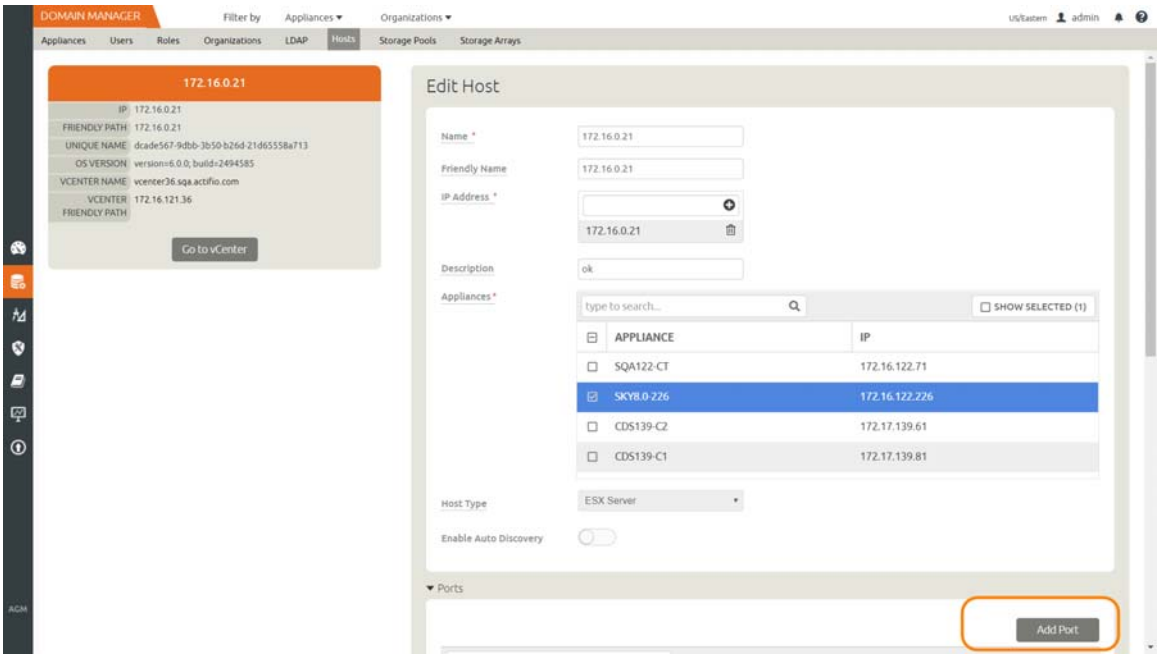
Adding the iSCSI IBM InfoSphere Definition to the ESX server

1. Highlight the ESX server in vCenter and select the **Configuration** tab.
2. Select the iSCSI Software Adapter and then **Properties**. A pop up window appears to discover the IBM InfoSphere iSCSI connection.
3. Select Dynamic Discovery tab and click **Add** to add the iSCSI IP of the InfoSphere VDP Appliance.
4. Enter the IP address of the IBM InfoSphere iSCSI port and click **OK**. It is added to the target listing.
5. Right click on the iSCSI software adapter and click **Rescan**.

Continue to Configuring IVGM to See the ESX Host on page 21.

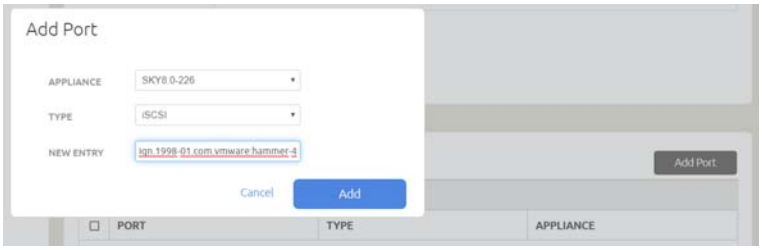
Configuring IVGM to See the ESX Host

1. Open IVGM to the **Domain Manager**, Hosts page.
2. Right-click the ESX server and select **Edit**.
3. Scroll down the right side to the Ports section and click **Add Port**



Configuring IVGM to Recognize an ESX Server

4. From the Type menu, select **iSCSI**.
5. At New Entry, enter the iSCSI iqn name, and click **Add**. This will configure the iSCSI relationship on IBM InfoSphere to the ESX server.



Adding the Port

Specifying the NIC for NFS mounts

Specify the NIC for an NFS mount at the ESX level:

```
udstask chhost -nfsoption server:serverip=1.1.1.1 <hostid>
```

The -nfsoption parameter is detailed in the ***VDP CLI Reference***.

Ensuring iSCSI Connectivity on a Linux Host

When the VDP Connector manages data movement over iSCSI, VDP uses a staging disk to create a copy of application data during each Snapshot or Dedup Async job.

Learning iSCSI information from a Linux Host

An IBM InfoSphere-approved iSCSI initiator must be installed on the host.

To learn if the initiator is installed, use this command:

```
[root@psa-611 ~]# grep -v ^# /etc/iscsi/initiatorname.iscsi | cut -d "=" -f 2
iqn.1994-05.com.redhat:6d11e98139fb
[root@psa-611 ~]# iscsiadm -m discovery
172.25.128.200:3260 via sendtargets
```

Installing the iSCSI Initiator on a Red Hat RHEL 6 or CentOS Linux Host

To install the iSCSI initiator on a Linux host:

Make sure you have the iscsiadm package installed.
Run: # `rpm -qa | grep iscsi`

This should show something similar to: `iscsi-initiator-utils-6.2.0.865-6.el5.x86_64.rpm`

If you see nothing, then you must install the package: # `yum install iscsi-initiator-utils`

Installing the iSCSI Initiator on a SLES Linux Host

Use YaST to install the iSCSI initiator package.

Make sure you have the `open-iscsi` package installed.
Run: # `rpm -qa | grep iscsi`

This should show something similar to:
`open-iscsi-x.x.x.x`
`yast2-iscsi-client-x.x.x.x`

If you do not see both of these packages, then you must install open-iscsi:

1. `# yast2 sw_single`
2. In the search, enter `iscsi`
3. Select `open-iscsi` and click **Accept**.

Ensuring iSCSI Connectivity on an IBM AIX Host

The InfoSphere VDP Appliance must be able to communicate with the VDP Connector running on the new host over a Fibre Channel or iSCSI network.

When Fibre Channel is not available, you can use iSCSI. If iSCSI is used, then an IBM InfoSphere-approved iSCSI initiator must be installed on the host. While it is possible to also present the staging disk to a VM using an iSCSI initiator running in the VM, this is normally not necessary.

To Learn the iSCSI Initiator Name from an AIX Host

To learn the name of the iSCSI initiator already installed on a host:

```
bash-4.2# lsattr -El iscsi0| grep -i "initiator_name" | awk '{print $2;}'
iqn.localhost.hostid.7f000001
```

Validating that the iSCSI Initiator is Installed on an IBM AIX Host

To determine if the iSCSI initiator is installed on an AIX host:

```
[bigblue4:root] / > lslpp -l | grep iscsi
  devices.common.IBM.iscsi.rte
  devices.iscsi.disk.rte 7.1.0.15  COMMITTED  iSCSI Disk Software
  devices.iscsi.tape.rte 7.1.0.0  COMMITTED  iSCSI Tape Software
  devices.iscsi_sw.rte 7.1.1.15  COMMITTED  iSCSI Software Device Driver
  devices.common.IBM.iscsi.rte
  devices.iscsi_sw.rte 7.1.1.15  COMMITTED  iSCSI Software Device Driver
[bigblue4:root] / >
```

Note: *Inband devices (VDisks) presented to the AIX host via iSCSI must have the* `rw_timeout` *attribute set to 120 seconds.*

Ensuring vSCSI Connectivity on an IBM HMC Host

Limitations

IBM HMC hosts can be added to an IBM InfoSphere VDP Appliance for LPAR discovery, but VDP Appliances do not support Fibre Channel connectivity, so the LPARs must be presented to their staging disks over an iSCSI connection.

Ensuring Connectivity

LPAR hosts with vSCSI mapping are virtual hosts that rely on VIO servers for vSCSI connectivity. They do not have direct FC connectivity and FC is not an option for them. If they are discovered as regular physical hosts, then the only option to back them up is using iSCSI, which is inferior to vSCSI. For enabling vSCSI connectivity with this class of LPARs:

- They must be discovered indirectly through HMC discovery, not directly as regular physical hosts.
- The InfoSphere VDP Appliance should have Fibre Channel connectivity to VIO servers catering storage to these LPARs.

If either of these two conditions are not met, the appliance will use iSCSI connectivity.

Resources such as RAM and CPU are still managed by the HMC but I/O such as network and fibre are managed through the VIO server. This is more scalable than earlier technologies. LUN presentation is done through the HBA cards on the VIO server(s). The VIO server presents the LUNs in a virtual SCSI mapping manner to the LPAR or vhost.

Because the VDP Connector has direct ties with the HMC of the environment, VDP can protect and recover vSCSI VIO mapped LPARS from an environment including the rootvg in a bootable state.

When the VDP Connector manages data movement over vSCSI, VDP uses a staging disk to create a copy of application data during each Snapshot or Dedup Async job.

Ensuring iSCSI Connectivity on a Solaris Host

The InfoSphere VDP Appliance must be able to communicate with the VDP Connector running on the new host over a Fibre Channel or iSCSI network.

When the VDP Connector manages data movement over iSCSI, VDP uses a staging disk to create a copy of application data during each Snapshot or Dedup Async job.

Connecting to Solaris x86 Hosts over iSCSI

To learn the iSCSI initiator Name from a Solaris x86 Host, use this command:

```
root@solaris5531:~# iscsiadm list initiator-node | grep -i "Initiator node name" | cut -d
":" -f 2,3
iqn.2015-02.com.actifio:solaris5531
```

Make sure you have the iSCSI package installed:

```
# pkginfo |grep SUNWiscsi
  system      SUNWiscsir                      Sun iSCSI Device Driver (root)
  system      SUNWiscsiu                      Sun iSCSI Management Utilities (usr)
```

Installing the pkg File

To install the iSCSI Initiator package on a Solaris Host:

```
# pkgadd -d <path_to_pkg_file> all
```

Solaris iSCSI Initiator Limitations

Here are the current limitations or restrictions of using the Solaris iSCSI initiator software:

- Support for iSCSI devices that use SLP is not currently available.
- Boot support for iSCSI devices is not currently available.
- iSCSI targets cannot be configured as dump devices.
- iSCSI supports multiple connections per session, but the current Solaris implementation only supports a single connection per session. For more information, see RFC 3720.
- Transferring large amounts of data over your existing network can have an impact on performance.

Ensuring iSCSI Connectivity on an HP-UX Host

When the VDP Connector manages data movement over iSCSI, VDP uses a staging disk to create a copy of application data during each Snapshot or Dedup Async job.

If iSCSI is used, then an IBM InfoSphere-approved iSCSI initiator must be installed on the host. While it is possible to also present the staging disk to a VM using an iSCSI initiator running in the VM, this is normally not necessary.

Note: *After the iSCSI initiator is configured, the HP-UX native multipathing is statically linked with the kernel, so no setup is required to use the multipathing support.*

Ensuring iSCSI Connectivity on a Windows Physical Host

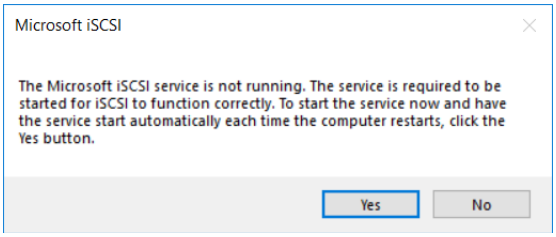
Windows Server hosts include Microsoft SQL Server, SharePoint, and Exchange hosts, as well as Active Directory, CIFS, and other file systems.

When the VDP Connector manages data movement over iSCSI, VDP uses a staging disk to create a copy of application data during each Snapshot or Dedup Async job.

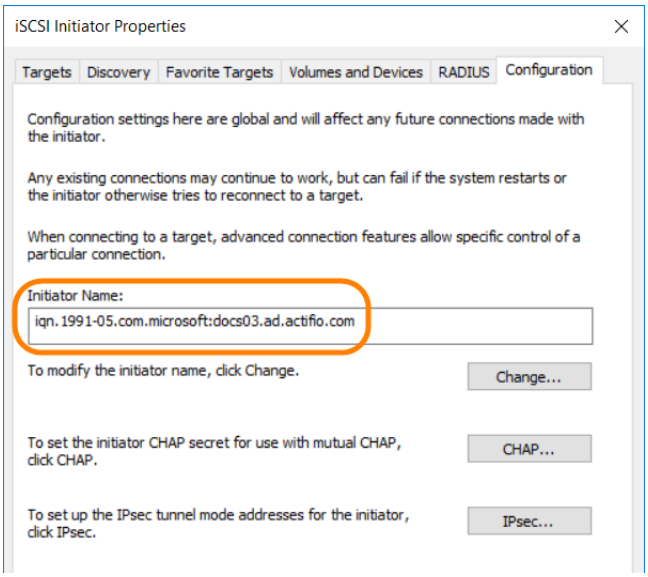
An IBM InfoSphere-approved iSCSI initiator must be installed on the host. While it is possible to also present the staging disk to a VM using an iSCSI initiator running in the VM, this is normally not necessary.

Learn the iSCSI Initiator Name from a Physical Windows Host via Server Manager

1. On Windows Server 2012, 2012 R2, or 2016, open up Server Manager.
2. Click Tools and select iSCSI Initiator to start the MSiSCSI Initiator Service.
3. The Microsoft iSCSI dialog will open indicating that the service is not running. Click Yes to start the service and to set it to start automatically when the server reboots.



4. After the MSiSCSI Initiator Service has started the Properties dialog will be opened. Click the Configuration tab to retrieve the iSCSI Qualified Name (IQN).
5. Write down or copy the Initiator Name.



Learn the iSCSI Initiator Name from a Physical Windows Host via the CLI

To learn the iSCSI initiator name from a physical Windows host, use the iscsicli command:

```
C:\Users\Administrator>iscsicli
Microsoft iSCSI Initiator Version 6.0 Build 6000
[iqn.1991-05.com.microsoft:winsql2016-1.sqa.actifio.com] Enter command or ^C to exit
```

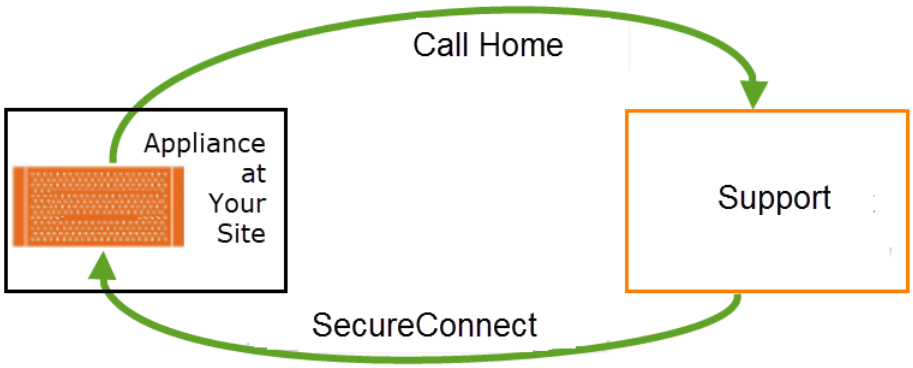
You will need this value when you add the host to the InfoSphere VDP Appliance.

5 IBM InfoSphere Remote Support

IBM InfoSphere offers two optional remote support features:

Call Home remote event notification: When you enable the Call Home feature, your InfoSphere VDP Appliance sends alerts and other diagnostic data to IBM InfoSphere. IBM InfoSphere Customer Support engineers monitor system alerts and conduct impact assessments. Based upon the alert level, the system may even initiate a problem resolution case and an associated escalation plan for you.
IBM InfoSphere Call Home is detailed in IBM InfoSphere Call Home Remote Event Notification.

SecureConnect remote service access: When you enable SecureConnect, IBM InfoSphere Customer Support engineers can access your system remotely on an as-needed basis. As a situation requires, they can manage major upgrades and service pack updates and hotfixes, phase out failing hardware, collect log data on history of failures, restart data and I/O modules, change the configuration of ports, and more. All actions are documented in the VDP audit log and in the IBM InfoSphere installation/problem reporting databases for further review.
IBM InfoSphere SecureConnect is detailed in IBM InfoSphere SecureConnect on page 29.



Call Home and SecureConnect

IBM InfoSphere Call Home Remote Event Notification

IBM InfoSphere Call Home sends an email to IBM InfoSphere Customer Support every six hours. In the event of a problem, IBM InfoSphere Support can refer to this information to minimize time to recovery. The email includes these statistics:

- VDP version information
- Uptime of the InfoSphere VDP Appliance
- Status check of services
- Process summary
- Logs of various processes
- Failed jobs and total jobs
- Storage pool and deduplication statistics

IBM InfoSphere Customer Support engineers monitor system alerts and conduct impact assessments. Based upon the alert level, the system may even initiate a problem resolution case and an associated escalation plan for you.

As of v9.0 release, IBM InfoSphere is offering customers an optional HTTPS Call Home capability that enables the Customer Success team to proactively identify and remediate potential issues. It can also be used to generate the Insight reports available through InfoSphere VDP. In prior releases, the IBM InfoSphere Call Home data could only be sent using email over SMTP. The HTTPS transport is often more reliable and simpler to configure than SMTP.

Can I Enable Call Home Without Enabling SecureConnect?

Yes. Call Home provides data, and SecureConnect provides access. Enabling Call Home without enabling SecureConnect ensures that IBM InfoSphere Customer Support has excellent monitoring, alerting, and analytics data, without the access that might be needed to perform further diagnostics or remediation. The data lets IBM InfoSphere Customer Support know when a problem has occurred and prepare a response if needed, but investigation and troubleshooting has to be performed via WebEx or conference call.

Most investigations require additional data to be gathered from the appliance, and without SecureConnect, the cycle of gather-analyze-followup-analyze can become cumbersome.

Call-Home Network Requirements

IBM InfoSphere Call Home uses HTTPS or SMTP. The port numbers for these configurations will depend on your own network setup. The default port numbers are: 25 for SMTP, 443 for HTTPS.

> ***Note:*** *Access to the Call Home web site* https://callhome.actifio.net *should never be blocked by your firewall.*

An IBM InfoSphere Administrator must configure the InfoSphere VDP Appliance to communicate with an SMTP/HTTPS/proxy server as detailed in ***Configuring Event Alerting***.

Configuring IBM InfoSphere Call Home

To send InfoSphere VDP Appliance statistics to IBM InfoSphere Support every 6 hours, refer to the IVGM online help, reachable from the **?** icon in the top right corner of the IVGM.

IBM InfoSphere SecureConnect

IBM InfoSphere SecureConnect is a secure method for remote support that employs dedicated ports and encrypted data. These built-in security features greatly reduce the risks associated with a connection to an external network. The SecureConnect protocol allows IBM InfoSphere Customer Support engineers to access your system on an as-needed basis to manage cases and updates while meeting your SLA requirements.

Your IBM InfoSphere account team is kept up to date on a repair status as the case progresses. If hardware replacement is required, parts & local support are shipped to the site and an IBM InfoSphere Services engineer is dispatched to handle the installation. When the incident is resolved to your satisfaction, the IBM InfoSphere Customer Support engineer logs out of your InfoSphere VDP Appliance, disconnects from the remote access line, and creates a summary report of problem root cause and repair actions that is delivered to your account team and to you.

Advantages to using IBM InfoSphere SecureConnect include:

- **Accelerated problem solving**: By leveraging IBM InfoSphere follow-the-sun support, you can resolve problems without extending the wait time that invariably gets generated by relying on log files, dumps, and traces being transmitted across the globe.
- **Fine-grained monitoring and collaboration**: You can monitor remote support activities and join in conference calls with IBM InfoSphere Customer Support engineers as the problem determination process proceeds.
- **Real-time learning**: Remote IBM InfoSphere Customer Support engineers provide you with ongoing assistance in the setup, configuration, and management of your InfoSphere VDP Appliances.

Without SecureConnect enabled, you can still contact IBM InfoSphere Customer Support. IBM InfoSphere support engineers can work with you via WebEx and other remote support tools for log file gathering and other forensics to help resolve the issue.

Can I Enable SecureConnect Without Enabling Call Home?

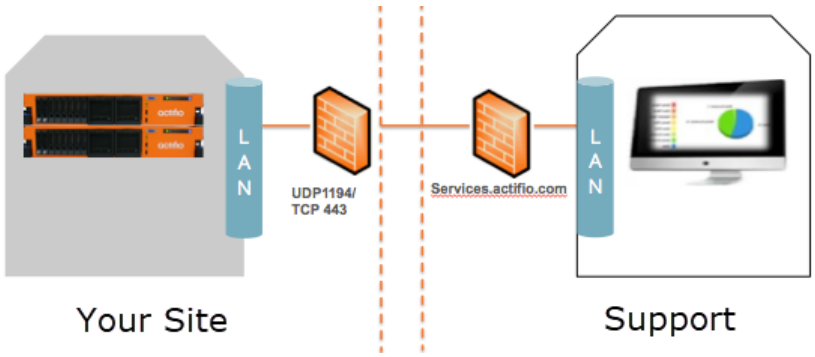
Yes. Call Home provides data, and SecureConnect provides access. Enabling SecureConnect without enabling Call Home allows IBM InfoSphere Customer Support engineers to respond and investigate issues after you tell us a problem exists. Without Call Home, IBM InfoSphere Customer Support has no way to know of problems with your system. There is no proactive data collection associated with activating SecureConnect.

How SecureConnect Works

SecureConnect uses client/server architecture. The SecureConnect client comes built into your InfoSphere VDP Appliances, to be enabled and disabled by you.

After you enable the connection through IVGM, your InfoSphere VDP Appliance establishes a secure point-to-point connection to a secure server at the IBM InfoSphere Global Support Center, enabling remote access from the IBM InfoSphere Global Support Center to your InfoSphere VDP Appliance. You must configure a firewall rule to allow the InfoSphere VDP Appliance to connect over UDP on port 1194.

As a client connection, SecureConnect does not bridge networks or perform any form of routing. Connections initiated at the IBM InfoSphere Global Support Center communicate with your InfoSphere VDP Appliance and no other systems on your network.



How Secure Is IBM InfoSphere SecureConnect?

SecureConnect utilizes 2048-bit RSA cryptography for strong mutual authentication and encryption, 256-bit AES for encryption of data in flight, and Diffie-Hellman for Perfect Forward Secrecy (PFS) key exchange. Each connection is a point-to-point link and none of your equipment can access another endpoint. Intrusion detection software continually monitors the connection for any anomalous activity. Authentication records are replicated in real-time to off-site locations. The SecureConnect servers are routinely monitored for emerging threats and vulnerabilities.

Only select users within the support and engineering organizations are authorized with this level of access. IBM InfoSphere employees who have a business need to access your systems must pass a third-party background check and sign a security, compliance, and confidentiality agreement. Access is reviewed annually and terminated immediately in the event of separation or role change. Authorized employees authenticate to SecureConnect with a 2048-bit X.509 certificate stamped with the identity of the user. A two-factor challenge is required after cryptographic authentication in the form of a smart phone push or code-generating token. The certificate must be renewed annually. Issuance is logged to an audit log, and all activities on a system while logged in using the certificate are logged along with the identity of the user. The VPN connection is protected using NIST-approved strong cryptography including AES-256 data encryption.

No Access to Your Business Data

Appliance service credentials are completely independent from SecureConnect and are generated on entirely separate systems. To gain access to a customer system, an IBM InfoSphere Support staff member generates a time-limited, passphrase-protected authentication token which is locked specifically to the machine they have been granted access to log into. The system generating these tokens is on a secure network separate from the SecureConnect network and itself authenticates against a robust corporate directory. The ability to generate authentication tokens is limited to IBM InfoSphere Support staff members who have been approved by a rigorous screening process.

IBM InfoSphere SecureConnect Network Requirements

IBM InfoSphere SecureConnect is a strong 2048-bit RSA mutually authenticated service not subject to redirection or man-in-the-middle attacks. SecureConnect requires a UDP connection over port 1194 **from** the InfoSphere VDP Appliance IP address **to** secureconnect2.actifio.com and a setting of “any” IP address. If you cannot use ‘any’, then contact IBM InfoSphere Support.

Enabling IBM InfoSphere SecureConnect

To enable SecureConnect mode, refer to the IVGM online help, reachable from the **?** icon in the top right corner of the IVGM.