Installation Guide

Dell EMC Integrated Data Protection Appliance DP4400

Version 2.2

302-004-957
REV. 03
June 2019

DELL EMC

Installation overview

This guide is designed for personnel who install, configure, and maintain the Integrated Data Protection Appliance DP4400. To use this hardware publication, you should be familiar with digital storage equipment and cabling.

Before you begin

Gather the required materials and configure your network environment as specified in Prepare the site and unpack the system on page 3.

Use the following sequence of actions as a guide to install the system.

Procedure

1. Install and secure the rails.
2. Install the system in the cabinet and attach the bezel.
3. Connect the system to the network.
4. Connect the power cables and power on.

Results

The system is ready for initial configuration. To continue setup, refer to the *Integrated Data Protection Appliance DP4400 Getting Started Guide*. For additional help and resources, review the information in Additional resources on page 17.

Prepare the site and unpack the system

Before you begin

Verify that you have the following components:

- 2U DP4400 system
- Rail kit, including:
  - Two sliding rails
  - Two velcro straps
  - Four screws
  - Four washers
- Two power cables
- Bezel
- Phillips-head screwdriver with magnetic tip (not provided)
- Two Cat 5e or Cat 6 copper Ethernet cables
- Four qualified 10 Gb Ethernet cables:
  - Fibre cables with a 10 Gb optical SFP
  - Direct-attached copper cables
- Anti-static wrist strap and conductive foam pad
- A VGA monitor with a keyboard or a computer with a serial port/usb-serial adapter and an appropriate cable for setting up iDRAC.

You must have a computer at the install location with:

- A power adapter, C13 to NEMA 5–15 (if based in North America or country specific cord in other geographical locations), or a power cord for your laptop power adapter with a C13 plug, to power your laptop from a rack PDU
- An Ethernet port
- Latest version of Google Chrome or Mozilla Firefox

Note

The DP4400 supports only one network. Separate management, backup, or replication network configurations (such as VLAN tagging) are not supported.

The following steps must be completed before starting initial configuration with the Appliance Configuration Manager:

Procedure

1. Identify 14 unassigned IP addresses for the IDPA components. To simplify configuration, you must select 14 contiguous addresses.

   Note that all components must run on a single VLAN or subnet with the exception of the iDRAC interface, which can be on a separate subnet or VLAN. For further information about IP addresses, see Table 1 on page 4.

2. Register the 14 IP addresses in DNS with forward and reverse lookup entries for each address. Ensure that the router for the 14 IP addresses can be pinged.

   See IP address breakdown on page 4 for more information.

3. Download the license files for Data Domain Virtual Edition (DDVE), Avamar Virtual Edition (AVE), and Data Protection Advisor (DP Advisor) from the Dell EMC Software Licensing Central.

   The contact person mentioned on your sales order should have received the License Authorization Code (LAC) letter through an email during the order fulfillment process. The LAC letter includes the license authorization code associated with your order, instructions for downloading software binaries, and instructions for activating the entitlements online through Dell EMC Software Licensing Central.

   Follow the steps mentioned in the LAC letter to activate the software and download the license keys. For additional information, see the Standard Activation Process section in the *License Activation Guide*.

   Note

   The LAC letter has the link `https://licensing.emc.com/deeplink/<LAC>` which directs you to Dell EMC Software Licensing Central. *<LAC>* is a unique alphanumeric value that is mentioned in your LAC letter.

   After the activation is complete, download the license keys that are generated for Data Domain Virtual Edition (DDVE), Avamar Virtual Edition (AVE), and Data Protection Advisor (DP Advisor). Use these license keys during the IDPA configuration.

IP address breakdown

When a range of IP addresses is used during the IDPA configuration, the IP addresses are assigned in a standard order. Use the following table to determine which IP address is allocated to a component.

The first column in each table, IP Range Allocation, is the value to add to the first IP address in the range. The **Sample Hostname** column is only a suggested naming convention.

Table 1 IP address range assignments

IP Range Allocation	Component	Description	Sample Hostname
+0	vCenter	VMware vCenter Server VM	idpa-vc.domain.local
+1	Data Domain	Data IP 1	idpa-dd1.domain.local
+2	Data Domain	Data IP 2	idpa-dd2.domain.local
+3	Data Domain	Data IP 3	idpa-dd3.domain.local
+4	Avamar	Server IP	idpa-av.domain.local
+5	Avamar	Avamar Proxy VM	idpa-avproxy.domain.local
+6	IDPA System Manager	IDPA System Manager VM	idpa-sysmgr.domain.local
+7	Data Protection Advisor	Application Server Host VM	idpa-dpa1.domain.local

Table 1 IP address range assignments (continued)

IP Range Allocation	Component	Description	Sample Hostname
+8	Data Protection Advisor	Datastore Server Host VM	idpa-dpa2.domain.local
+9	Data Protection Search	Index Master Node Host VM	idpa-search.domain.local
+10	DD Cloud DR CDRA (optional)	Data Domain Cloud Disaster Recovery (DD Cloud DR) Cloud DR Add-on (CDRA) virtual appliance	idpa-cdra.domain.local

The following three IP addresses are required for additional connectivity, but are not configured as a part of the range.

Table 2 Additional IP addresses

Component	Description	Sample Hostname
ESXi	VMware ESXi	idpa-esxi.domain.local
Appliance Configuration Manager (ACM)	ACM VM	idpa-acm.domain.local
iDRAC (optional)	Integrated Dell Remote Access Controller	idpa-idrac.domain.local

Install Network Validation Tool

The Network Validation Tool (NVT) runs multiple tests to validate the network configuration. You need to run the NVT from a system on the management network.

Before you install IDPA, it is recommended that you run the Network Validation Tool to validate the network settings for a successful deployment of IDPA in the datacenter. You must review the network configuration before starting the IDPA installation. To download the NVT and for more information about the tool, see https://help.psapps.emc.com/display/HELP/Network+Validation+Tool+for+IDPA.

Install the rails

The rails are labeled left and right, and cannot be interchanged. The front side of each rail is labeled **Left Front** or **Right Front** when the rail faces the cabinet front.

Procedure

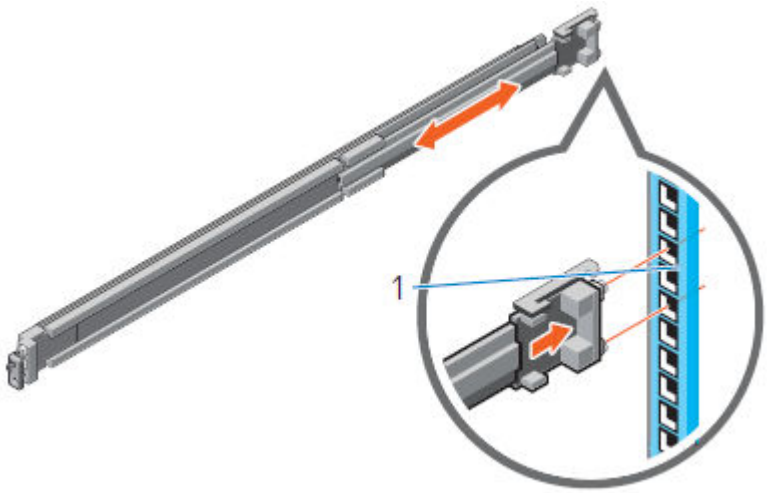
1. Determine where to mount the system, and mark the location at the front and back of the cabinet.

   Note

   Install the left rail assembly first.

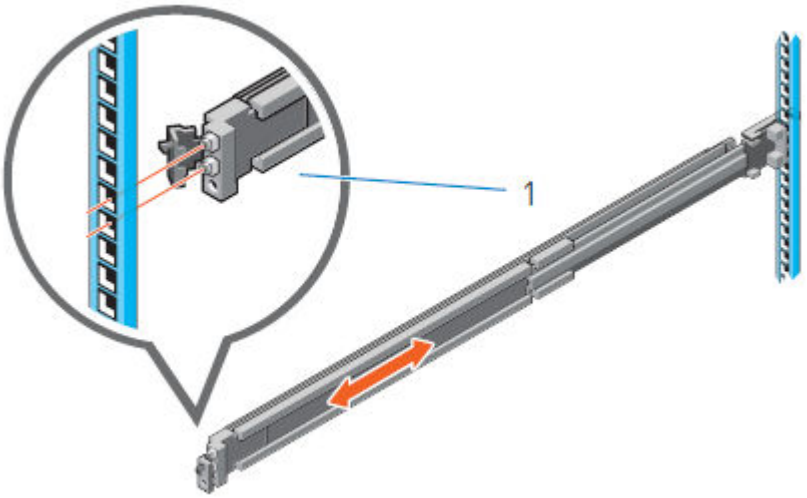
2. Fully extend the rear sliding bracket of the rail.
3. Position the rail end piece labeled **Left Front** facing inward and orient the rear end piece to align with the holes on the rear cabinet flanges.
4. Push the rail straight toward the rear of the rack until the latch locks in place.

Figure 1 Installing the rear end of the rail



5. For the front end piece, rotate the latch outward and pull the rail forward until the pins slide into the flange, and release the latch to secure the rail in place.

Figure 2 Installing the front end of the rail



6. Repeat the preceding steps to install the right rail assembly.

Secure the rails to the cabinet

The supplied screws and washers are used to secure the rail assemblies to the front and rear of the cabinet.

Note

For square hole cabinets, install the supplied conical washer before installing the screw. For unthreaded round hole cabinets, install only the screw without the conical washer.

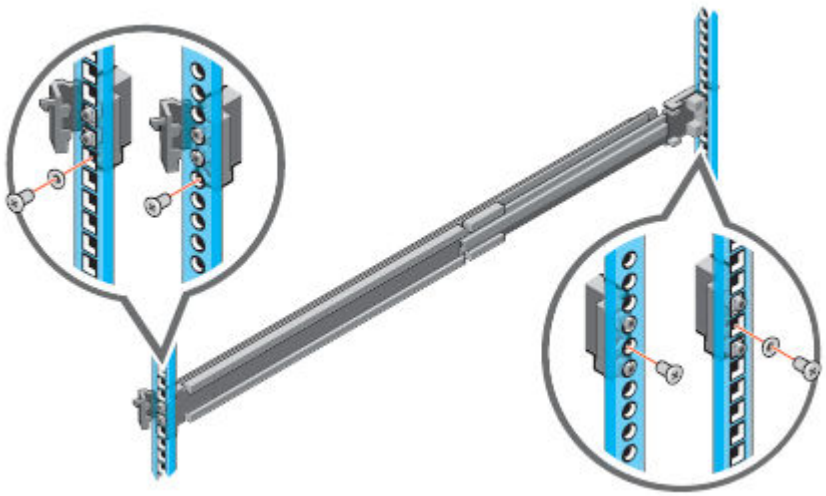
Procedure

1. Align the screws with the designated U spaces on the front and rear rack flanges.

   Ensure that the screw holes on the tab of the system retention bracket are seated on the designated U spaces.

2. Insert and tighten the two screws using the Phillips #2 screwdriver.

   Figure 3 Installing screws



Install the system in the cabinet

⚠WARNING

The system is heavy and should be installed in a cabinet by two people. To avoid personal injury and/or damage to the equipment, do not attempt to install the system in a cabinet without a mechanical lift and/or help from another person.

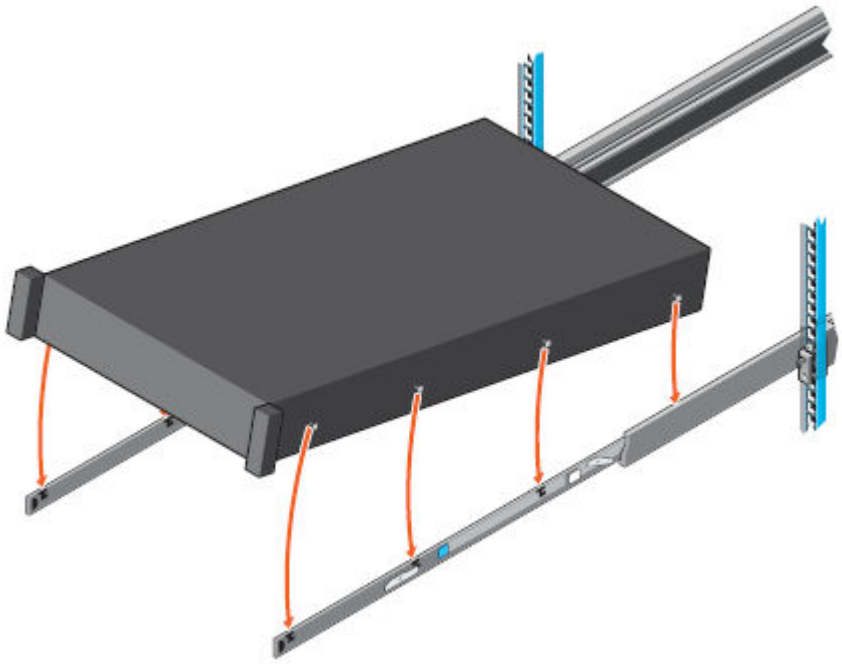
Procedure

1. At front of the cabinet, pull the inner slide rails out of the cabinet until they lock into place.

Figure 4 Pull the inner rails out of the cabinet

2. Locate the rear rail standoff on each side of the system. Position the system above the rails and lower the rear rail standoffs into the rear J-slots on the slide assemblies.
3. Rotate the system downward until all the rail standoffs are seated in the J-slots.

Figure 5 Install the system in the rails

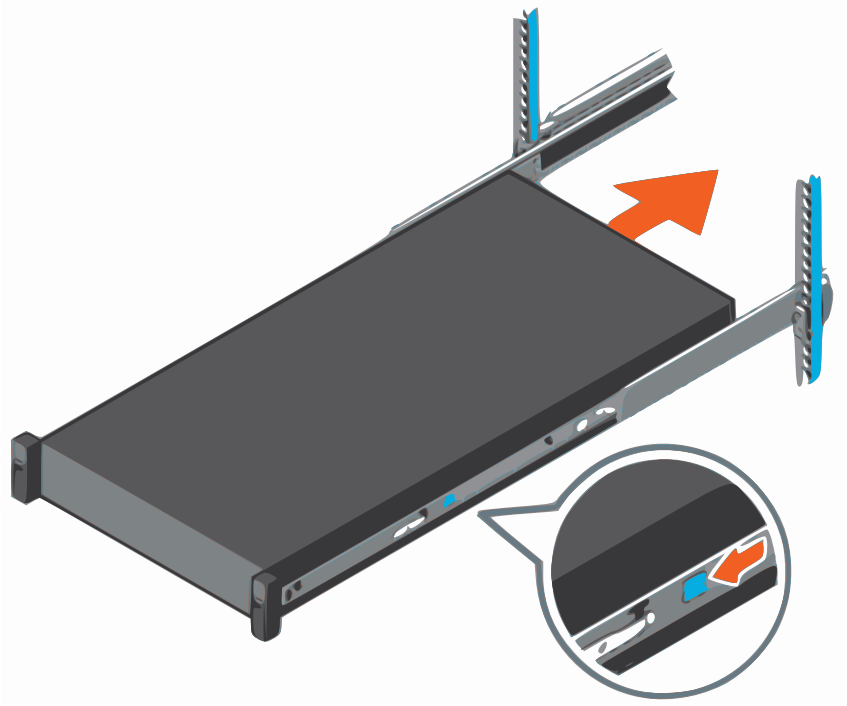


4. Push the system inward until the lock levers click into place.
5. Pull the blue slide release lock tabs forward on both rails and slide the system into the cabinet. The slam latches will engage to secure the system in the cabinet.

Note

Ensure that the inner rail slides completely into the middle rail. The middle rail locks if the inner rail is not fully engaged.

Figure 6 Slide the system into the cabinet

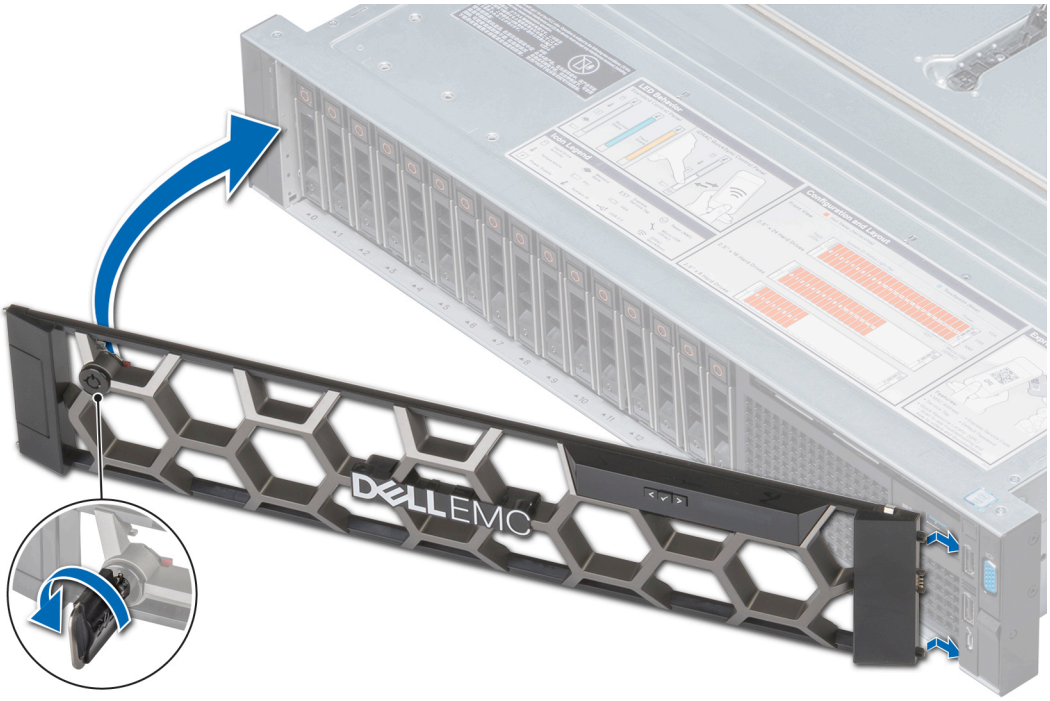


Install the bezel

Procedure

1. Align and insert the right end of the bezel onto the system.
2. Press the release button and fit the left end of the bezel onto the system.
3. Lock the bezel by using the key.

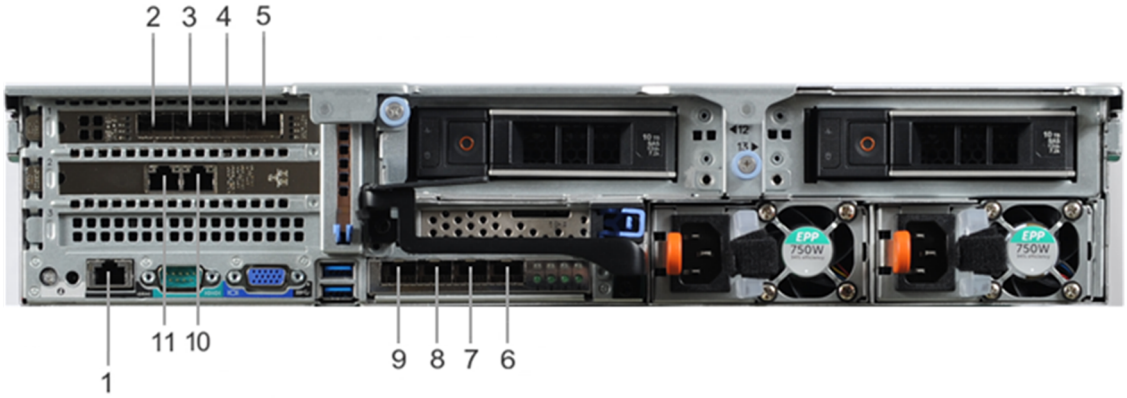
Figure 7 Installing the front bezel



Connect the system to the network

The following figure shows the location of the DP4400 network ports and iDRAC port.

Figure 8 DP4400 network and iDRAC connections



Procedure

1. Use a Cat 5e or Cat 6 copper Ethernet cable to connect a 1 GbE port (10) to the service computer.
2. Use Fibre cables with a 10 Gb optical SFP, 1GBaseT RJ-45, or direct-attached copper cables to connect the four required 10 GbE ports (2, 3, 8, 9) to access ports on the switch in your network.
3. Use a Cat 5e or Cat 6 copper Ethernet cable to connect the iDRAC port (1) in the lower left of the system chassis to the network.

DP4400 ports

The following table provides the port type for the DP4400 ports.

Table 3 DP4400 port types

Callout number	Port type
1	iDRAC
2	10 GbE (required)
3	10 GbE (required)
4	10 GbE (unused)
5	10 GbE (unused)
6	10 GbE (unused)
7	10 GbE (unused)
8	10 GbE (required)
9	10 GbE (required)
10	1 GbE
11	1 GbE (unused)

Note

Ports 2 and 9 are a vSwitch0 network team. Ports 3 and 8 are a vSwitch1 network team and are used during appliance configuration.

Note

Uplink ports are not trunking ports.

Note

Ensure that the four required 10 GbE ports (2, 3, 8, and 9) are connected to the access ports on the switch in your network.

Connect the power cables and power on

Procedure

1. Connect the power supply units to the rack.

   Note

   For dual PSU systems, connect each PSU to a redundant AC power source. Redundant power sources allow one AC source to fail or be serviced without impacting system operation. Connect PSU 0 to one AC source, and PSU 1 to the other AC source.

The system may not power on automatically after plugging in the AC power cords. The system identification button located on the rear of the chassis, on the lower left-hand side illuminates blue when power is on.

2. If the system does not power on automatically after connecting the power cables, press the power button on the right control panel at the front of the chassis to power on the system .

Configure iDRAC

The IDPA systems require that the Integrated Dell Remote Access Controller (iDRAC) is configured for system upgrade and maintenance operations. Additionally, the systems support the use of iDRAC to change security settings and enables to remotely power the system on and off.

Before you begin

Connect to the unit using a VGA monitor with a keyboard or a serial port, power on the appliance, and perform the following steps:

Note

Do not use iDRAC to change the storage configuration, system settings, or BIOS settings, as making changes to these will impact the system functionality. Contact Support if changes are required in any of these areas.

Procedure

1. During the system boot process, press **F2** to access the BIOS menu.
2. In the **System Setup Main Menu** page, click **iDRAC Settings**.

   The iDRAC Settings page is displayed.
3. Click **Network**.

   The Network page is displayed.
4. Under **IPv4 Settings**, specify static IP address details.
5. Press **Esc** to return to the previous menu.
6. Select **User Configuration**.
   a. Enable the root user.
   b. Change the root user password.

      Note that the default password is *Idpa_1234*.

Installing the DataProtection-ACM pre-installation patch

Before you configure the DataProtection-ACM virtual machine, install the latest IDPA pre-installation patch if it is available.

For example:

`Idpa_pre_update_N.N.N-nnnnnn.tar.gz`

Where *N.N.N* is the latest pre-installation patch version and *nnnnnn* is the build number.

You can install the pre-installation patch when the DataProtection-ACM is not registered with Secure Remote Services gateway by using SSH.

Install the IDPA pre-installation patch on the DataProtection-ACM

Before you begin

Before you configure the DataProtection-ACM virtual machine, install the latest IDPA pre-installation patch if it is available.

For example:

`Idpa_pre_update_N.N.N.nnnnnn.tar.gz`
Where:

- *N.N.N* is the latest pre-installation patch version.
- *nnnnnn* is the build number.

You can install the pre-installation patch when the DataProtection-ACM is not registered with ESRS gateway by using SSH.

Procedure

1. Check https://support.emc.com/downloads/41849_Integrated-Data-Protection-Appliance to see if a pre-installation patch is available for your version of IDPA. If a pre-installation patch is available, download it to a folder on your laptop.

   For example:

   `Idpa_pre_update_N.N.N.nnnnnn.tar.gz`
   Where:

   - *N.N.N* is the latest pre-installation patch version.
   - *nnnnnn* is the build number.

2. Open the WinSCP or SCP application on the service laptop, and then connect to the DataProtection-ACM by performing the following actions:

   a. In the **File protocol** field, select **SFTP**.

   b. In the **Hostname** field, enter `192.168.100.100` as the IP address of the DataProtection-ACM.

   c. In the **Port number** field, specify the default port number **22**.

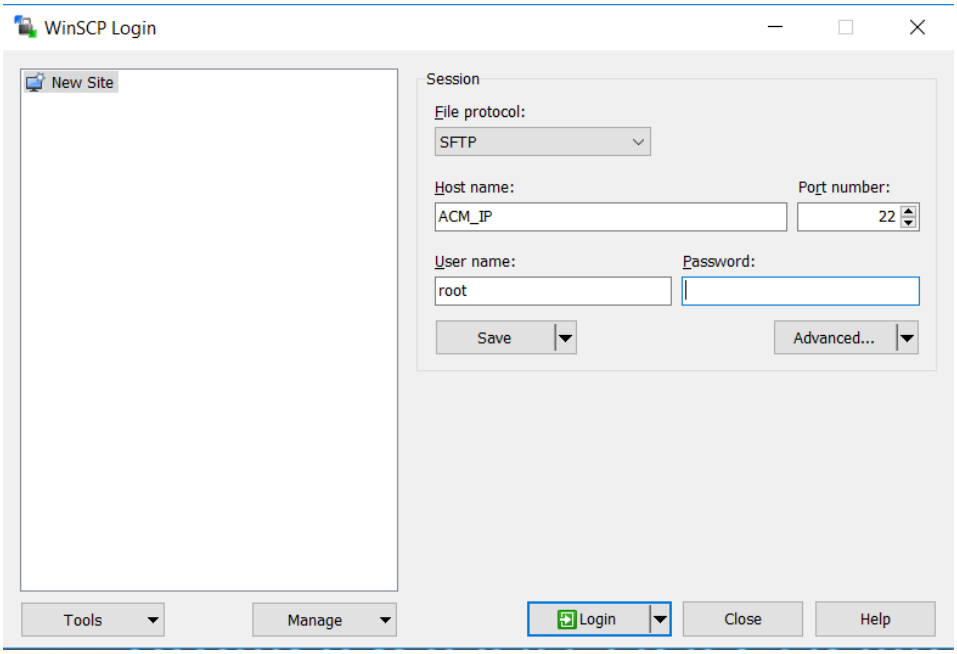
   d. In the **User name** field, enter `root`.

   e. In the **Password** field, enter `Idpa_1234`.

   f. Click **Login**.

   The following figure shows a sample WinSCP session configuration window.

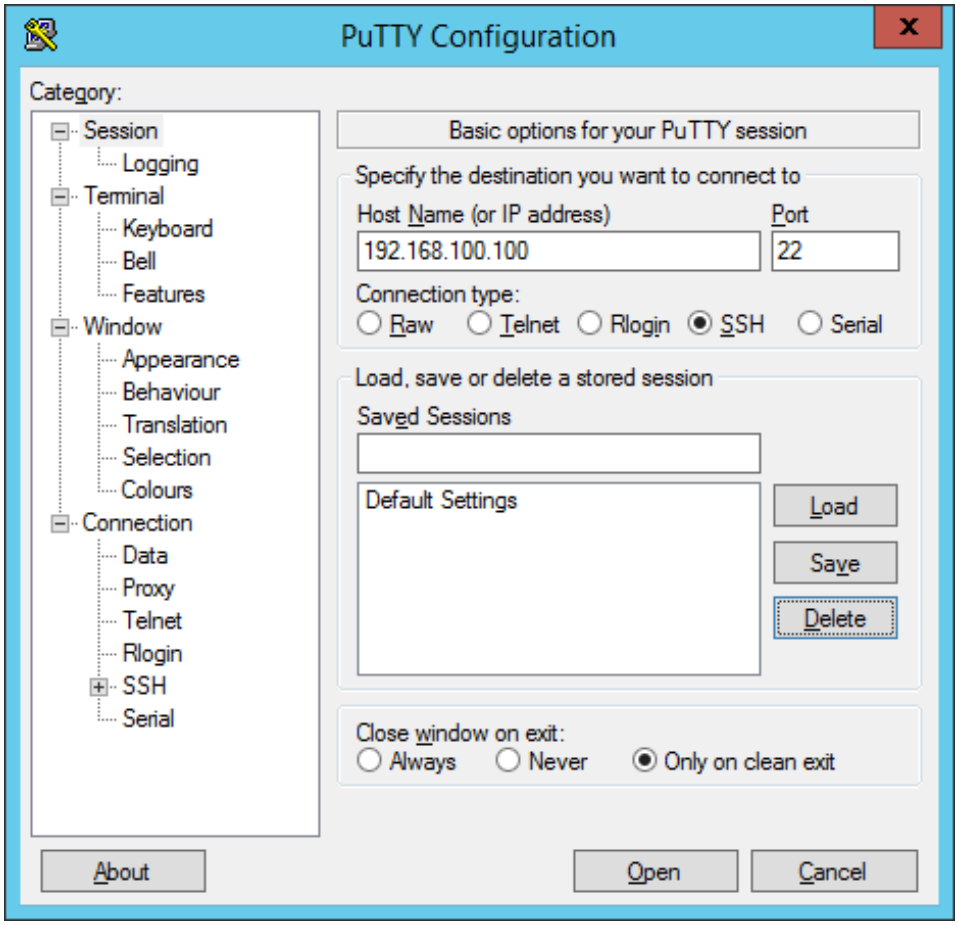
Figure 9 WinSCP session configuration window



3. Create a temporary folder `/tmp/patch`.
4. Copy the `Idpa_pre_update_N.N.N.nnnnnn.tar.gz` file to the `/tmp/patch` directory.
5. Connect to the DataProtection-ACM by using Putty from the service laptop.

   The following figure shows the Putty configuration screen.

Figure 10 Putty Configuration screen for DataProtection-ACM



6. At the login as prompt, type **root**.
7. At the Password prompt, type the password for the root user.

   The default password for the root user is Idpa_1234.
8. Determine the DataProtection-ACM version by typing the following command:

   rpm -qa | grep dataprotection
   Ensure that the DataProtection-ACM version is earlier than *dataprotection-2.0.0-571095.x86_64*.
9. Change to the directory that contains the pre-installation patch file by typing the following command:

   cd /tmp/patch
10. Extract the contents of the `.tar.gz` file by typing the following command:

    tar -xvf `Idpa_pre_update_N.N.N.nnnnnn.tar.gz`

    The contents are extracted to a subdirectory named `Idpa_pre_update_N.N.N.nnnnnn`.
11. Change directory to `Idpa_pre_update_N.N.N.nnnnnn.tar.gz` directory by typing the following command:

    cd /tmp/patch/Idpa_pre_update_*N.N.N.nnnnnn*/
12. Change permission of `install.sh` file by typing the following command:

chmod +x install.sh

13. Run the installation script file by typing the following command:

    ./install.sh

    Messages be displayed on the screen during the installation process. The following message might be displayed, which you can ignore:

    "warning: file /usr/local/dataprotection/var/configmgr/server_data/config/InfrastructureComponents_Template.xml: remove failed: No such file or directory"
    "warning: file /usr/local/dataprotection/customscripts/Config.properties: remove failed: No such file or directory"

14. Verify that the pre-installation patch installation completed successfully by typing the following command:

    rpm -qa | grep dataprotection
    Ensure that the DataProtection-ACM version is *dataprotection-2.0.0-571095.x86_64* or later.

15. Delete the `Idpa_pre_update_N.N.N.nnnnnn.tar.gz` file, and then delete the `/tmp/patch/Idpa_pre_update_N.N.N.nnnnnn` directory.

16. Edit the `/usr/local/dataprotection/server/version/applianceVersion.xml` file and modify value in the <build> tag to the latest build for the ACM and IDPA nodes.

    The following example highlights the changes that you must make to the <build> tag. In this example, the build number is 571095.

```
<applianceVersion>
    <id>IDPA</id>
    <version>
        <major>2</major>
        <subMajor>0</subMajor>
        <minor>0</minor>
        <build>571095</build>
    </version>
    <components>
        <component>
            <id>ACM</id>
            <version>
                <major>1</major>
                <subMajor>0</subMajor>
                <minor>0</minor>
                <build>571095</build>
            </version>
        </component>
```

Launch the Appliance Configuration Manager

The Appliance Configuration Manager (ACM) walks you through the steps to configure network settings, license the IDPA software, and configure the IDPA.

For more information about configuring the IDPA with the ACM, refer to the *Integrated Data Protection Appliance DP4400 Getting Started Guide*. This document

explains common user tasks such as how to create backup policies and restore from backup.

Additional resources

Document references for the IDPA

The IDPA documentation set includes the following publications:

- *Integrated Data Protection Appliance DP4400 Installation Guide*
  Instruction for installing the IDPA DP4400 hardware.
- *Integrated Data Protection Appliance DP4400 Getting Started Guide*
  Explains how to perform initial IDPA configuration tasks and how to get started with basic functionality like backup and restore.
- *Integrated Data Protection Appliance Product Guide*
  Provides the overview and administration information about the IDPA system.
- *Integrated Data Protection Appliance Release Notes*
  Product information about the current IDPA release.
- *Integrated Data Protection Appliance DP4400 Service Procedure Guide*
  Procedures for replacing or upgrading hardware components of the IDPA.
- *Integrated Data Protection Appliance Security Configuration Guide*
  Information about the security features that are used to control user and network access, monitor system access and use, and support the transmission of storage data.
- *Integrated Data Protection Appliance Software Compatibility Guide*
  Information about software components and versions used in the IDPA product.

IDPA training resources

Video walkthroughs, demonstrations, and explanations of product features are available online.

You can obtain additional IDPA training and information at https://education.emc.com, such as:

- Integrated Data Protection Appliance 2.2 DP4400 Overview
- Integrated Data Protection Appliance 2.2 DP4400 Getting Started
- Integrated Data Protection Appliance 2.2 DP4400 CRU Maintenance
- Integrated Data Protection Appliance 2.2 System Manager Overview
- Integrated Data Protection Appliance 2.2 Alert Monitoring

Published June 2019