Microsoft Windows Server Staging

- Drive Partition Guidelines, on page 1
- Windows Setup Guidelines, on page 2
- Join Standalone Servers to Domain in Microsoft Windows Server , on page 3
- Set Persistent Static Routes, on page 4
- Collect Existing SNMP Properties, on page 4
- Display Settings, on page 6
- System Properties, on page 6
- Configure Event Viewer, on page 7
- Connectivity Validation, on page 7

Drive Partition Guidelines

Create drive partitions for the servers being built according to settings in the Unified ICM/Cisco Unified Contact Center Enterprise System Design Specification.

Format C drive as NTFS.

Note You might need to use the manufacturer's drive partitioning/RAID array software to set up the partition.

Logger or Administration and Data Server Partition Guidelines

For servers hosting a Logger or Administration & Data Server (Historical Data Server (HDS)), use the following guidelines for partitioning:

- Use the C drive for the operating system, virtual memory paging file size, core Unified ICM, Microsoft SQL Server, and Microsoft SQL Server log and temp files.
- Use the D drive to store the Logger or Historical Data Server database.

Note Keep the Microsoft SQL Server temp and log files on the C drive to maximize database performance.

Partition Guidelines for Other Contact Center Components

For servers hosting a Router, Peripheral Gateway, Administration & Data Server (non-Historical Data Server), CTI Server, and CTI OS Server, use a single partition C drive for the operating system, virtual memory paging file size, core Unified ICM software, the Administration & Data Server database, Microsoft SQL Server, and Microsoft SQL Server log and temp files.

Windows Setup Guidelines

Note For additional information on installing and upgrading Microsoft Windows Server, see the Microsoft Windows Server homepage.

Use the following guidelines when setting up a Microsoft Windows Server for Unified ICM:

- When setting the time zone, ensure that all Central Controller systems are set for the same time zone regardless of their physical location.
- Ensure that the time zone is set the same on PG A and PG B for all peripheral gateway pairs to enable synchronization of Unified ICM Message Delivery Service (MDS) processes.
- For Network Settings, enter the server respective IP and DNS data according to the System Design Specification.
- For the Public Ethernet Card, perform the following tasks:
  - To enter the data for visible IP addresses, subnet mask, default gateway and preferred and alternate DNS servers for the server, click **Start** > **Control Panel** > **Network and Sharing** > **Change Adapter Settings** and then right-click on the Visible network **Properties** > **Internet Protocol version 4 (TCP/IPV4)**, and select **Properties**.
  - In the **Advanced** tab, enter the “high” visible addresses.
  - In the **DNS** tab, for **DNS suffix for this connection**, enter the name of the local DNS zone for the server and check **Register**.
  - If the server requires access to resources in a different trusting or trusted domain or DNS zone, select **append these DNS suffixes (in order)** and enter the local DNS zone for the server first, then add the other secondary zones which represent the trusting or trusted domain.
- If the server has more than one network interface card, for the Private Ethernet Card click **Start** > **Control Panel** > **Network and Sharing** > **Change Adapter Settings**, right-click on the Private network and select **Properties**, and perform the following tasks:
  - Uncheck the **Client for Microsoft Networks** and the **File and Print Sharing** options.
  - For TCP/IP properties, enter the private IP address and subnet mask for the server. Leave the default gateway field blank.
  - In the Advanced tab, enter the “high” private addresses.
  - In the DNS tab, leave the address space empty and uncheck **Register**.

- Because the ICM platform does not directly support IP V6, disable IPV6 on all the Ethernet cards. On the **Adapter Settings** dialog, right-click the card and select **Properties**. Uncheck **Internet Protocol Version 6 (TCP/IPV6)**.

Related Topics

Enable SNMP Management on Microsoft Windows Server, on page 3

Enable SNMP Management on Microsoft Windows Server

Unified ICM/CCE SNMP support automatically installs during setup—you do not need to take extra steps during setup to enable SNMP support. The Microsoft Windows SNMP service is disabled as part of web setup and is replaced by the Cisco Contact Center SNMP Management service to process SNMP requests in its place.

However, you must install Microsoft Windows SNMP optional components on Unified ICM/CCE servers for any SNMP agents to function. The Microsoft SNMP components are required for Cisco SNMP support. You must install these Microsoft SNMP components before you install any Unified ICM/CCE components that require SNMP monitoring.

To install Microsoft SNMP components:

Procedure

Step 1 Choose **Start** > **Control Panel** and then click **Programs and Features**.

Step 2 Click **Turn Windows features on or off**.
The **Server Manager** opens, followed by the **Add Roles and Features Wizard**.

Step 3 Click **Next** to proceed through the wizard until you reach **Select Features**.

Step 4 In the **Features** list, select **SNMP Service** and **SNMP WMI Provider**.

Step 5 Click **Next**, and then click **Install**.

Join Standalone Servers to Domain in Microsoft Windows Server

The following components must be installed on servers that are members of the domain:

- Logger
- CallRouter
- Administration & Data Servers

Procedure

Step 1 Click Start, right-click **Computer** and choose **Properties**.

Step 2 In the section “Computer name, domain, and workgroup settings” click **Change settings**.

Step 3 Click **Change**.

Step 4 In the “Member of” section, select **Domain** then enter the Fully Qualified Domain Name and click **OK**.

Step 5 Enter the Domain Administrator's username and password.

Step 6 Reboot the server and sign in to the domain.

Set Persistent Static Routes

For geographically distributed Central Controller sites, redundant CallRouter, Logger, and Peripheral Gateway components typically have a Private IP WAN connection between Side A and Side B. Windows only allows one default gateway for each VM (which sends the Private Network traffic to the Public Network). So, you add a Static Route to all the VMs running the CallRouter, Logger, and PG applications.

To create a persistent static route with the **route add** command, you need the destination subnet, the subnet mask, the local gateway IP, and the interface number of the local Private Network interface:

```
route add <destination subnet> mask <subnet mask> <gateway IP> IF <interface number> -p
```

Procedure

Step 1 On each CallRouter, Logger, or PG VM, run `ipconfig /all`.
Record the `IPv4 Address`, `Subnet Mask`, and `Physical Address` (MAC address) for the Private Network interface.

Step 2 On each of these VMs, run `route print -4`.
Record the `Interface` for the Private Network. You can identify the correct interface by looking for its `Physical Address` (MAC address).

Step 3 On each of these VMs, run `route add <destination subnet> mask <subnet mask> <gateway IP> IF <interface number> -p` to add a persistent static route for the remote Private Network.

Collect Existing SNMP Properties

If you already installed and configured SNMP management support for this server, collect the existing configuration parameters so you can use them to configure the components installed by Web Setup. You can find these parameters on the property sheets associated with the Microsoft SNMP Service.

Note For Microsoft Windows Server, to view the SNMP Agent Management snap-in, use the 32-bit Microsoft Management Console Snap-In. To launch the 32-bit Snap-in, run mmc /32. For detailed instructions for Microsoft Windows Server, consult your Microsoft documentation.

To collect existing SNMP properties:

Procedure

Step 1 On the Services MMC console, do one of the following:

- Locate and select the **SNMP Service** in the list, or
- Choose **Start** > **Programs** > **Control Panel** > **Administrative Tools** > **Services**.

Step 2 On the SNMP Service Properties dialog box, select the **Security** tab.

Note the following settings and configuration data:

- The state of the **Send authentication trap** check box.
- The Accepted community names.
- If **Accept SNMP packets from these hosts** is checked, collect the host names or IP addresses configured in the associated list box.

  Note To configure Cisco SNMP agents if you configured host names (versus IP addresses), determine the actual IP address of that host. For security reasons, using static addresses for management stations is preferred.

Step 3 Select the **Traps** tab on the SNMP Service Properties dialog box.

Collect the configured trap destinations and the associated community name.

Note If host names were for trap destinations, determine the actual IP address of that host.

Step 4 On the SNMP Service Properties dialog box, select the **Agent** tab.

Collect the information from the Contact and the Location fields.

What to do next

If the server has not been configured for SNMP manageability, do the following:

1. Determine whether SNMP manageability is required.
2. Acquire the necessary configuration information to enable SNMP access.

The necessary configuration information includes:

- The IP addresses of the management station.
- If using SNMP v1 or SNMP v2c:
  - Community names (if using SNMP v1 or SNMP v2c)
  - Trap destinations and the community name expected by each management station
- If using SNMP v3:
  - Usernames
  - Authentication protocol used (if authentication is required)
  - Privacy protocol used (if privacy is required)

- Trap destinations and the username expected by each management station

The installed Microsoft Management Console Snap-In (Cisco SNMP Agent Management) is used to configure the SNMP properties. See the *SNMP Guide for Cisco Unified ICM/Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html for more details.

Display Settings

Through the Windows Control Panel Display dialog box:

- Ensure that no screen saver is selected.
- Set the Administration & Data Server display for at least 1024 by 768 pixel resolution.
- Set at least 65K colors and at least 60 MHz.

System Properties

For Virtual memory settings:

- Click **Start** > **Control Panel** > **System** > **Advanced System Settings** > **Performance** > **Advanced** > **Virtual Memory**.
- Next, select **Change** and set the initial and maximum page file sizes to appropriate values based on the system memory. See Microsoft documentation for guidance on page file sizes.

Note Microsoft recommends the paging file size to be at least 1.5 times the VM memory.

For Startup and Recovery settings:

- Click **Start** > **Control Panel** > **Advanced System Settings** > **Startup and Recovery** > **Settings**.
- Next, set the value of the **Time to display list of operating systems** to **3** seconds.

Note Click **Start** > **Control Panel** > **System** > **Advanced System Settings** > **Performance** > **Advanced**. Confirm that the **Adjust for best performance** option is set to either **Programs** or **Background Services**.

Configure Event Viewer

Procedure

Step 1 For each type of event, set the **Maximum log size** to **8192 KB**.

Step 2 Select **Overwrite events as needed**.

Note See the Security Guide for Cisco Unified ICM/Contact Center Enterprise available at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-technical-reference-list.html for additional information.

Connectivity Validation

Before you begin the Unified ICM installation process, validate network connectivity for all servers that are part of the Unified ICM system.

On each server:

- Validate the TCP/IP properties for each network card, including the DNS settings.
- Validate that you can ping each machine on the visible network.
- If applicable, validate that you can ping each private network connection.
- Test remote access.

Related Topics

System Design Specification