Other Security Considerations

Other Cisco Call Center Applications

The following sections discuss security considerations for other Cisco Call Center applications.

Cisco Unified ICM Router

The file **dbagent.acl** is an internal, background file. Do not edit this file. However, this file must have the READ permission set, so that the file can allow users to connect to the router's real-time feed.

Peripheral Gateways (PGs) and Agent Login

There's a rate limit of Unified CCE agent login attempts with incorrect password. By default, the agent account is disabled for 15 minutes after three incorrect password attempts, counted over a period of 15 minutes.

You can change this default by using registry keys. The registry keys are under: `HKLM\SOFTWARE\Cisco Systems, Inc.\\ICM\<inst>\PG(n)[A/B]\PG\CurrentVersion\PIMS\pim(n)\EAGENTData\Dynamic`

The registry keys include the following:

- **AccountLockoutDuration:** Default

After the account is locked out because of unsuccessful login attempts, this value is the number of minutes the account remains locked out.

- **AccountLockoutResetCountDuration:** The default is 15. Number of minutes before the AccountLockoutThreshold count goes back to zero. This is applicable if the account doesn't get locked out, but you have unsuccessful login attempts less than the value mentioned in AccountLockoutThreshold.
- **AccountLockoutThreshold:** The default is 3. This is the number of unsuccessful login attempts after which the account is locked out.

Note These settings are applicable only on Desktop solutions other than Cisco Finesse, such as CTI OS with a System Peripheral Gateway.

Finesse blocks access to user accounts, if agents or supervisors try to sign in to the desktop five times consecutively with a wrong password. The lockout period is five minutes. For more information about these settings, see the *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html.

When Single Sign-On (SSO) is enabled for an agent, the account lockout mechanism is managed by the associated identity provider.

Endpoint Security

Agent Desktops

Cisco Finesse supports HTTPS (TLS 1.2 only) for the Administration Console and agent and supervisor clients.

Unified IP Phone Device Authentication

When designing a contact center enterprise solution, you can implement device authentication for the Cisco Unified IP Phones. Contact center enterprise solutions support Unified Communications Manager's Authenticated Device Security Mode, which ensures the following:

- **Device Identity**—Mutual authentication using X.509 certificates
- **Signaling Integrity**—SIP messages authenticated using HMAC-SHA-1
- **Signaling Privacy**—SIP message content encrypted using AES-128-CBC

Media Encryption (SRTP) Considerations

Before enabling SRTP in your deployment, consider the following points:

- To use secure media on the agent leg, ensure that the installed IP phones are compatible with SRTP.
- The Virtualized Voice Browser supports SRTP for the VRU leg.
- The IOS VXML Gateway does not support SRTP.
- Mobile Agents cannot use SRTP.

- The Cisco Outbound Option Dialers do not support SRTP. While calls are connected to the Dialer, the calls cannot use SRTP. But, calls can negotiate SRTP once the call is no longer connected to the Dialer.

IP Phone Hardening

With the IP phone device configuration in Unified CM, you can disable certain phone features to harden the phones. For example, you can disable the phone's PC port or restrict a PC from accessing the voice VLAN. Changing some of these settings can disable the monitoring and recording features of the contact center enterprise solution. The settings are defined as follows:

- **PC Voice VLAN Access**—Indicates whether the phone allows a device attached to the PC port to access the Voice VLAN. Disabling Voice VLAN Access prevents the attached PC from sending and receiving data on the Voice VLAN. It also prevents the PC from receiving data sent and received by the phone. Disabling this feature disables desktop-based monitoring and recording.

  This setting is Enabled (the default).

- **Span to PC Port**—Indicates whether the phone forwards packets transmitted and received on the Phone Port to the PC Port. To use this feature, enable PC Voice VLAN access. Disabling this feature disables desktop-based monitoring and recording.

  This setting is Enabled.

Disable the following setting to prevent man-in-the-middle (MITM) attacks. Some third-party monitoring and recording applications use this mechanism for capturing voice streams.

- **Gratuitous ARP**—Indicates whether the phone learns MAC addresses from Gratuitous ARP responses.

  This setting is Disabled.

Vulnerability Scan and Penetration Test Considerations

Keep in mind the following considerations when you are performing the vulnerability scans and penetration test in your deployment:

- Cisco recommends that you perform the vulnerability scan and penetration test during off-peak times and maintenance windows on the production system.
- When you install patches for Maintenance Releases (MRs) or Engineering Specials (ES) for Unified ICM and Unified CVP, older versions of files that are included in the patch are backed up. You need these older versions of the files to be restored if you choose to uninstall the MR or ES patches for any reason. These older versions that are backed-up are not used by the software running on your computer and they do not pose any security threat. If you receive any software vulnerability notification on these backed-up folders or files, treat them as False Positive and define rules to suppress them. Details on the backup folders and file locations are available in the rollback files (Rollback_ICM_*.txt and Rollback_CVP_*.txt) inside each of the patch information folder:
  - For Unified ICM—PatchInfo_ICM_* within <install_drive>\icm
  - For Unified CVP—Patchinfo_CVP_* within <install_drive>\Cisco\CVP

Note You can delete the files in the backup folders. However, ensure to take a backup of these files if you need to roll back.

Java Upgrades

During installations and upgrades, Unified CCE installs the required base Java version.

Before updating the Java Runtime Environment (JRE):

- Export the certificates of all the components imported into the truststore.

  The command to export the certificates is *keytool -export -keystore <JRE path>\lib\security\cacerts -alias <alias of the component> -file <filepath>.cer*
- Enter the truststore password when prompted.

During installations and upgrades, Unified CCE installs the required base Java version. Oracle can release Java updates with important security fixes after you install your contact center. You can apply Java updates to your contact center as follows:

- You can apply Java updates for the latest 32-bit Java 8 minor version.

  For the most current Java support information, see the *Contact Center Enterprise Compatibility Matrix* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html.
- Modify the Windows JAVA_HOME path variable to point to the new Java Runtime Environment (JRE) location if it has changed.

After updating the OpenJDK Java Runtime Environment (JRE):

- Import the certificates for all the components that you previously exported from the truststore before you updated the JRE.

  The command to import certificates is *keytool -import -keystore <JRE path>\lib\security\cacerts -file <filepath>.cer -alias <alias>*.
- Enter the truststore password when prompted.
- Enter 'yes' when prompted to trust the certificate.

Upgrade Tomcat Utility

Use the optional Cisco Upgrade Tomcat Utility to:

- Upgrade Tomcat to version 7.0 build releases. (That is, only version 7.0 build releases work with this tool.) You may choose to upgrade to newer builds of Tomcat release 7.0 to keep up with the latest security fixes.

  Tomcat uses the following release numbering scheme: Major.minor.build. For example, you can upgrade from 7.0.62 to 7.0.65. You cannot use this tool for major or minor version upgrades.

- Revert a Tomcat upgrade.

  If upgrading Tomcat causes a problem, use the utility to revert to the previous release.

Note If you use the utility to upgrade Tomcat multiple times, you can revert to only one version back of Tomcat. For example, if you upgrade Tomcat from 7.0.62 to 7.0.63, and then to 7.0.75, the utility reverts Tomcat to 7.0.63.

Before using the tool:

- Download the Tomcat installer (apache-tomcat-version.exe) from the Tomcat website: http://archive.apache.org/dist/tomcat/tomcat-7/. Copy the installer onto the Unified CCE component VMs.
- Download the utility (UpgradeTomcatTool-<version>.jar) and copy it onto the Unified CCE component VMs.

  Download link: https://software.cisco.com/download/home/284360381/type/284416107/release/12.0(1).
- Delete or back up large log files in these directories to reduce upgrade time:

  c:\icm\tomcat\logs
  c:\icm\debug.txt

Upgrade Tomcat

For detailed information on the results from each step, see the ../UpgradeTomcatResults/UpgradeTomcat.log file.

Note Stop Unified CCE services on the VM before using the Tomcat Utility.

Procedure

Step 1 From the command line, navigate to the directory where you copied the Upgrade Tomcat Utility.

Step 2 Enter this command to run the tool: **java -jar UpgradeTomcatTool-<version>.jar -upgrade**

Step 3 When prompted, enter the full pathname of the new Tomcat installer.

For example:

```
c:\tomcatInstaller\apache-tomcat-<version>.exe
```

Step 4 When prompted, enter **yes** to continue with the upgrade.

Step 5 Repeat these steps for all unified CCE component VMs.

Revert Tomcat

For detailed information on the results from each step, see the ../UpgradeTomcatResults/UpgradeTomcat.log file.

Note Stop Unified CCE services on the VM before using the Tomcat Utility.

Procedure

Step 1 From the command line, navigate to the directory where you copied the Upgrade Tomcat Utility.

Step 2 Enter this command to run the tool: **java -jar UpgradeTomcatTool-<version>.jar -revert**

Step 3 When prompted, enter **yes** to continue with the reversion.

Step 4 Repeat these steps for all unified CCE component VMs.

Microsoft Security and Software Updates

Applying security and software update patches automatically from third-party vendors involves risk. Subtle changes in functionality or extra layers of code can alter the overall performance of Cisco Contact Center products.

Assess all security and software update patches released by Microsoft and install those patches deemed appropriate for your environment. Do not automatically enable Microsoft Windows Update. The update schedule can conflict with other Unified ICM/Unified CCE activity. Consider using Microsoft Software Update Service or similar patch management products to selectively apply Critical and Important security and software update patches. Follow the Microsoft guidelines about when and how you apply these updates.

Note Assess the security exposure of the critical security patches or cumulative updates that are released by Microsoft for Windows Operating System , IIS, and SQL. Apply critical security patches or cumulative updates as you deem necessary for your site.

Refer to *Cisco Customer Contact Software Policy for Third-Party Software/Security Updates* at https://www.cisco.com/c/en/us/products/contact-center/unified-contact-center-enterprise/bulletin-listing.html

Microsoft Internet Information Server (IIS)

Internet Script Editor requires Internet Information Server (IIS). Disable the service on any other node except for the Distributor. There are some exceptions for the multimedia configuration of the solution. In that case, follow the product documentation and system requirements.

Active Directory Deployment

This section describes the Active Directory Deployment topology. For more detailed Active Directory (AD) deployment guidance, consult the *Staging 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-guides-list.html.

While you can deploy your solution in a dedicated Windows Active Directory domain, it is not a requirement. Instead, you can use Organizational Units to deploy security principles. This closer integration with AD and the power of security delegation means that your corporate AD directories can house application servers (for domain membership), user and service accounts, and groups.

Global Catalog Requirements

Contact center enterprise solutions use the Global Catalog for Active Directory. All domains in the AD Forest in which the Unified CCE Hosts reside must publish the Global Catalog for that domain. This includes all domains with which your solution interacts, for example, Authentication, user lookups, and group lookups.

Note This does not imply cross-forest operation. Cross-forest operation is not supported.

Active Directory Site Topology

In a geographically distributed contact center enterprise solution, you locate redundant domain controllers at each of the sites. You establish a Global Catalog at each site to properly configure Inter-Site Replication Connections. Contact center enterprise solutions communicate with the Active Directory servers that are in their site. This requires an adequately implemented site topology in accordance with Microsoft guidelines.

Organizational Units

Application-Created OUs

When you install the solution software, the AD Domain in which the VMs are members must be in Native Mode. The installation adds several OU objects, containers, users, and groups for the solution. You need delegated control over the Organizational Unit in AD to install those objects. You can locate the OU anywhere in the domain hierarchy. The AD Administrator determines how deeply nested the contact center enterprise solution OU hierarchy is created and populated.

Note All created groups are Domain Local Security Groups, and all user accounts are domain accounts. The Service Logon domain account is added to the Local Administrators' group of the application servers.

The contact center enterprise installation integrates with a Domain Manager tool. You can use the tool standalone for preinstalling the OU hierarchies and objects required by the software. You can also use it when the Setup program is invoked to create the same objects in AD. The AD/OU creation can be done on the domain in which the running VM is a member or on a trusted domain.

Active Directory Administrator-Created OUs

An administrator can create certain AD objects. A prime example is the OU container for Unified CCE Servers. This OU container is manually added to contain the VMs that are members of a given domain. You move these VMs to this OU once they are joined to the domain. This segregation controls who can or cannot administer the servers (delegation of control). Most importantly, the segregation controls the AD Domain Security Policies that the application servers in the OU can or cannot inherit.

Related Topics

Windows Server Hardening

WMI Service Hardening

Windows Management Instrumentation (WMI) is used to manage Windows systems. WMI security is an extension of the security subsystem built into Windows operating systems. WMI security includes: WMI namespace-level security; Distributed COM (DCOM) security; and Standard Windows OS security.

WMI Namespace-Level Security

To configure the WMI namespace-level security:

Procedure

Step 1 Launch the `%SYSTEMROOT%\System32\Wmimgmt.msc MMC` control.

Step 2 Right-click the **WMI Control** icon and select **Properties**.

Step 3 Select the **Security** properties page.

Step 4 Select the Root folder and click the **Security** button.

Step 5 Remove EVERYONE from the selection list then click the **OK** button.

Only give ALL rights to <machine>\Administrators.

More WMI Security Considerations

The WMI services are set to **Manual** startup by default. Third-Party Management agents use these services to capture system data. Do not disable WMI services unless required.

Perform DCOM security configuration in a manner that is consistent with your scripting environment. Refer to the WMI security documentation for more details on using DCOM security. For information on securing a remote WMI connection, see the Microsoft Developer Network article: http://msdn.microsoft.com/en-us/library/aa393266%28v=vs.85%29.aspx.

SNMP Hardening

Refer to the *SNMP Guide for Cisco Unified ICM/Contact Center Enterprise* for details on installation, setting the community names, usernames, and trap destinations.

Although the Microsoft Management and Monitoring Tools subcomponents are necessary for SNMP manageability, the Web Setup tool disables the Microsoft SNMP service. A more secure agent infrastructure replaces the Microsoft SNMP service. Do not re-enable the Microsoft SNMP service. It can cause conflicts with the Cisco-installed SNMP agents.

Explicitly disable the Microsoft SNMP trap service. Do not run management software for collecting SNMP traps on contact center servers. This restriction makes the Microsoft SNMP trap service unnecessary.

Versions 1 and 2c of the SNMP protocol are less secure than Version 3. SNMP Version 3 features a significant step forward in security. For contact center hosts located on internal networks behind corporate firewalls, enable SNMP manageability by applying the following configuration and hardening:

1. Create SNMP v1/v2c community strings or SNMP v3 usernames using a combination of upper, and lowercase characters. DO NOT use the common “public” and “private” community strings. Create names that are difficult to guess.
2. Use of SNMP v3 is highly preferred. Always enable authentication for each SNMP v3 username. The use of a privacy protocol is also encouraged.
3. Limit the number of hosts that are allowed to connect to SNMP manageable devices.
4. Configure community strings and usernames on manageable devices to accept SNMP requests only from those hosts running SNMP management applications. (This configuration is done through the SNMP agent configuration tool when defining community strings and usernames.)
5. Enable sending of SNMP traps for authentication failures. These traps alert you to potential attackers trying to “guess” community strings and usernames.

SNMP manageability is installed on contact center servers and is executing by default. However, for security reasons, SNMP access is denied until the previous configuration steps have been completed.

For greater security, you can configure IPsec filters and an IPsec policy for SNMP traffic between an SNMP management station and SNMP agents. Follow the Microsoft advice on how to configure the filters and policy. For more information on IPsec policy for SNMP traffic, see the Microsoft TechNet articles.

Toll Fraud Prevention

Toll fraud is a serious issue in the Telecommunications Industry. The fraudulent use of telecommunications technology can be expensive for a company, so the Telecom Administrator must take the necessary precautions to prevent fraud. For Unified CCE environments, resources are available at Cisco.com on how to lock down Unified CM systems and to mitigate against toll fraud.

In Unified ICM, the primary concern is in using dynamic labels in the label node of a Unified ICM script. If the dynamic label is constructed from information entered by a caller (such as with Run External Script), then constructing labels of the following form is possible:

- 9.....
- 9011....

- And similar patterns

These labels can send the call to outside lines or even to international numbers. Some dial plans configured in the routing client can allow such numbers to go through. If the customer does not want such labels used, then the Unified ICM script must check for valid labels before using them.

A simple example is an ICM script that prompts the caller with “If you know your party's extension, enter it now,”. The script then uses the digits entered blindly in a dynamic label node. This script might transfer the call anywhere. If you do not want this behavior, then either the Unified ICM routing script or the routing client's dial plan must check for and disallow invalid numbers.

An example of a Unified ICM script check is an “If” node that uses an expression such as:

```
substr (Call.CallerEnteredDigits, 1, 1) = "9"
```

The True branch of this node would then branch back to ask the caller again. The False branch would allow the call to proceed. This case is only an example. Each customer must decide what is and what is not allowed based on their own environment.

Unified ICM does not usually transfer calls to arbitrary phone numbers. Numbers have to be explicitly configured as legal destinations. Alternatively, the logic in the Unified ICM routing script can transfer the call to a phone number from a script variable. You can write scripts so that a caller enters a series of digits and the script treats it as a destination phone number, asking the routing client to transfer the call to that number. Add logic to such a script to make sure the requested destination phone number is reasonable.

Third-Party Security Providers

Cisco has qualified Unified ICM software with the Operating System implementations of NTLM, Kerberos V, and IPsec security protocols.

Cisco does not support other third-party security provider implementations.

Third-Party Management Agents

In their server operating system installations, some vendors include agents to provide convenient server management and monitoring.

Such agents can be valuable, but also impact performance. Cisco does not support their use on mission-critical Unified ICM/CCE servers.

Warning Configure agents in accordance to the antivirus policies described in this document. Do not run Polling or intrusive scans during peak hours, but rather schedule these activities for maintenance windows.

Note Install SNMP services as instructed by these third-party management applications to take full advantage of the management capabilities provided with your servers. Without SNMP, enterprise management applications do not receive hardware prefailure alerts. Unified CCE servers only support 32-bit extension agents.

Related Topics

General Antivirus Guidelines

Self-Encrypting Drives

With Unified CCE, you can deploy self-encrypting drives (SED) that have special hardware that encrypts incoming data and decrypts outgoing data in real-time. The encrypting and decrypting of data does not impact overall system performance.

A media encryption key on the disk controls the encryption and decryption of data. A security key also known as the Key-Encryption-Key or Authentication passphrase is used to encrypt the media encryption key. The security key can be provided locally by the user or remotely by using the KMIP server. If you lock the drive, no security key is required to retrieve the data.

For more information on SEDs, see the ***Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide*** https://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-c-series-integrated-management-controller/products-installation-and-configuration-guides-list.html.

The drives to be deployed must match the specifications for hard drives mentioned in the Virtualization Wiki. For more information, see https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-unified-contact-center-enterprise.html.